

# **BreezeNET PRO.11 Series**

## **User's Guide**



March 2003  
Software Version 5.1  
Cat. No. 213403

© 2002 by Alvarion Ltd. All rights reserved.

No part of this publication may be reproduced in any material form without the written permission of the copyright owner.

### **Trade Names**

BreezeACCESS®, BreezeNET®, BreezeLINK®, BreezeVIEW™, BreezeMANAGE™, BreezeCONFIG™, BreezeWIZARD™, BreezeSECURE™, AlvariBASE™, AlvariSTAR™, AlvariX™, WALKair® and WALKnet® are trade names or trademarks of Alvarion Ltd. Other brand and product names are trade names or trade marks of their respective owners.

### **Statement of Conditions**

The information contained in this manual is subject to change without notice. Alvarion Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

### **Warranties; Disclaimers**

All Alvarion Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

### **Exclusive Warranty**

Alvarion warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion's standard RMA procedure.

## **Disclaimer**

(a) UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

(c) ALVARION SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

### **Limitation of Liability**

(a) ALVARION SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

### **Electronic Emission Notices**

This device complies with Part 15 of the FCC rules, ETSI 300-328, UL, UL/C, TUV/GS, and CE.

Operation is subject to the following two conditions:

- 1.** This device may not cause harmful interference.
- 2.** This device must accept any interference received, including interference that may cause undesired operation.

### **FCC Radio Frequency Interference Statement**

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

# Important Notice

This user manual is delivered subject to the following conditions and restrictions:

- ◆ This manual contains proprietary information belonging to Alvarion Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion Ltd. products.
- ◆ No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Ltd.
- ◆ The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- ◆ The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.
- ◆ Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- ◆ Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

- ◆ The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.
- ◆ Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

Some of the equipment provided by Alvarion and specified in this manual, is manufactured and warranted by third parties. All such equipment must be installed and handled in full compliance with the instructions provided by such manufacturers as attached to this manual or provided thereafter by Alvarion or the manufacturers. Non-compliance with such instructions may result in serious damage and/or bodily harm and/or void the user's authority to operate the equipment and/or revoke the warranty provided by such manufacturer.

# Contacting Alvarion Technical Support

Should you need assistance beyond the scope of this guide, please contact your local Alvarion reseller or distributor. If they cannot solve your problem, feel free to contact the Alvarion Technical Support Department. The support representatives can assist you in solving any problems that cannot be solved by your reseller.

When requesting support, please have the following items available:

- ◆ Configuration of the system, including models of the Alvarion equipment used
- ◆ BreezeNET firmware version currently in use
- ◆ Antenna type and cable lengths
- ◆ Site information such as possible radio path problems (such as trees, machines, and buildings)
- ◆ Distance between devices
- ◆ Configuration, statistic counters, and error messages as seen on the monitor
- ◆ Description of problems encountered

To contact Alvarion Technical Support, refer to the Alvarion web site:  
<http://www.alvarion.com>.



# User's Guide



## Table of Contents

<b>Introduction .....</b>	<b>1-1</b>
<b>Scope of the Guide .....</b>	<b>1-2</b>
<b>BreezeNET PRO.11 Series Features .....</b>	<b>1-3</b>
<b>BreezeNET PRO.11 Series Product Line.....</b>	<b>1-5</b>
BreezeNET PRO.11 Access Point .....	1-6
BreezeNET PRO.11 Single Station Adapter .....	1-8
BreezeNET PRO.11 Four Port Station Adapter .....	1-10
BreezeNET PRO.11 Workgroup Bridge.....	1-12
BreezeNET PRO.11 SA-PCR Card .....	1-14
BreezeNET PRO.11 Extended Range Access Point and Bridge.....	1-15
<b>BreezeNET PRO.11 Functional Description .....</b>	<b>1-16</b>
Quick Review of Ethernet .....	1-16
Startup Procedure.....	1-16
AP-10 Access Point.....	1-17
SA-10 Station Adapter .....	1-17
SA-40 Station Adapter .....	1-18
WB-10 Wireless Bridge.....	1-18
SA-PCR Station Adapter .....	1-18

<b>Basic Installation .....</b>	<b>2-1</b>
<b>Basic Installation Checklist .....</b>	<b>2-2</b>
<b>Checking the Packing List .....</b>	<b>2-2</b>
<b>Positioning the Unit.....</b>	<b>2-3</b>
Metal Furniture .....	2-3
Microwave Ovens.....	2-3
Antennas.....	2-4
Heat Sources .....	2-4
Additional Considerations When Positioning the Access Point.....	2-4
<b>Connecting the Unit to the Power Supply.....</b>	<b>2-5</b>
<b>Connecting the Unit to the Ethernet Port .....</b>	<b>2-6</b>
<b>Checking Unit Functionality .....</b>	<b>2-7</b>
Station (SA-10, SA-40) and Bridge (WB-10) LEDs .....	2-7
Access Point LEDs .....	2-8
Verifying the Ethernet Connection .....	2-9
<b>Using the Local Terminal for Unit Setup and Management ..</b>	<b>3-1</b>
<b>Getting Started with the Local Terminal .....</b>	<b>3-3</b>
<b>Configuration Screens.....</b>	<b>3-4</b>
<b>Main Menu.....</b>	<b>3-12</b>
<b>System Configuration Menu .....</b>	<b>3-13</b>
Station Status .....	3-13
IP and SNMP Parameters .....	3-15
Wireless LAN (WLAN) Parameters.....	3-16
Bridging .....	3-20
Station Control.....	3-22
Security (Authentication Feature) .....	3-22

<b>Advanced Settings Menu.....</b>	<b>3-24</b>
Translation Mode .....	3-24
Roaming .....	3-25
Performance.....	3-26
Radio .....	3-28
Rate .....	3-29
AP Redundancy Support .....	3-29
Maintenance .....	3-29
Voice and Data Configuration .....	3-30
<b>Site Survey Menu .....</b>	<b>3-31</b>
System Counters.....	3-31
Survey Software .....	3-39
Using the Site Survey Software.....	3-39
Event Log.....	3-43
Display Neighboring APs .....	3-44
<b>Access Control Menu .....</b>	<b>3-44</b>
<b>Code Activate Control Menu .....</b>	<b>3-46</b>
 <b>SA-PCR PRO.11 PC Card Installation, Setup, and Management</b>	
<b>.....</b>	<b>4-1</b>
<b>Packing List .....</b>	<b>4-3</b>
<b>Before You Begin .....</b>	<b>4-3</b>
<b>Installing the SA-PCR Card .....</b>	<b>4-4</b>
Installing the SA-PCR Drivers.....	4-5
Checking the LED Indicators.....	4-20
Initial Configuration.....	4-21
<b>Installing the SA-PCR Utilities .....</b>	<b>4-22</b>
Installing the SA-PCR Driver for Windows 2000 Systems.....	4-23

<b>Using the SA-PCR Configuration Utility.....</b>	<b>4-28</b>
Station Status Tab.....	4-29
WLAN Parameters Tab.....	4-30
Station Control Tab .....	4-32
Configuration Access Tab .....	4-33
Power Management Tab.....	4-34
Security Tab.....	4-36
Maintenance Tab.....	4-38
Radio Tab .....	4-40
Performance Tab .....	4-41
Resetting the SA-PCR Card.....	4-42
Running the Configuration Utility with Windows 2000 .....	4-42
<b>Using the Windows CE SA-PCR Utility .....</b>	<b>4-45</b>
Configuration .....	4-45
Monitor .....	4-46
<b>Using the SA-PCR Site Survey Utility .....</b>	<b>4-48</b>
Accessing the SA-PCR Site Survey Utility.....	4-49
SA-PCR Site Survey Main Window .....	4-49
Performing a Site Survey with the SA-PCR.....	4-52
<b>Using the Upgrade Kit Program .....</b>	<b>4-54</b>
Upgrade Procedure for Windows 95/98 .....	4-54
Upgrade Procedure for Windows NT, DOS/ODI.....	4-60
<b>Installation Troubleshooting.....</b>	<b>4-61</b>
<b>Installing the SA-PCR Drivers in ODI Systems.....</b>	<b>4-62</b>
Configuration Notes.....	4-63
Running the Configuration Utility.....	4-63
Troubleshooting ODI Installation .....	4-64

<b>Installing the SA-PCR in Linux Systems .....</b>	<b>4-66</b>
Requirements .....	4-66
Installing the PCMCIA Package .....	4-67
Checking the SA-PCR Firmware Version in Linux.....	4-68
Installing the SA-PCR Linux Driver .....	4-69
Building the Driver.....	4-70
Configuration Steps Prior to Operation.....	4-72
SA-PCR Operation With Linux.....	4-75
 <b>BreezeCONFIG PRO.11 SNMP Configuration Utility .....</b>	 <b>5-1</b>
<b>Working with BreezeCONFIG PRO.11 .....</b>	<b>5-2</b>
Introducing the Configuration Utility Window .....	5-2
Working with the Toolbar Options .....	5-10
Working with the Menu Options.....	5-22
Working in Unit Configuration Mode .....	5-27
Working in Multiple Configuration Mode .....	5-28
Working with the Firmware Upgrade Utility.....	5-32
 <b>Working with Device Configurations .....</b>	 <b>5-37</b>
Station Status .....	5-38
IP Parameters.....	5-40
SNMP Parameters .....	5-41
WLAN Parameters .....	5-43
Station Control .....	5-47
Bridging (AP only).....	5-50
Security .....	5-52
Advanced Parameters.....	5-53
Counters.....	5-58

<b>Reading Trap Messages .....</b>	<b>5-63</b>
Accessing Trap Messages.....	5-63
Trap Table .....	5-64
<b>Planning and Installing Wireless LANs.....</b>	<b>6-1</b>
<b>System Configurations.....</b>	<b>6-2</b>
Single Cell Configuration .....	6-3
Overlapping Cell Configuration System Configurations .....	6-8
Multicell Configuration .....	6-11
Multi-Hop Configuration (Relay) .....	6-12
<b>Indoor Installation Considerations .....</b>	<b>6-15</b>
Site Selection Factors .....	6-15
Antennas for Indoor Applications.....	6-17
Construction Materials .....	6-19
Cell Size .....	6-20
<b>Outdoor Installation Considerations .....</b>	<b>6-21</b>
Site Selection Factors .....	6-21
Rooftop Installation .....	6-23
Antennas for Outdoor Applications.....	6-23
Antenna Seal.....	6-25
Cell Size .....	6-26
Link Distance .....	6-26
Using Outdoor Range Tables .....	6-27
FCC Outdoor Range Tables (USA) .....	6-27
ETSI Outdoor Range Tables (Europe and Rest-of-World) – D Models, DL Models.....	6-29
ETSI Outdoor Range Tables (Europe and Rest-of-World) – DE Models.....	6-31
Non-Regulated Outdoor Range Tables – D Models.....	6-32
Extending Range using the TPA-24 and LNA-10 .....	6-33

<b>Available Antennas and Antenna Kits.....</b>	<b>6-38</b>
<b>Precautions .....</b>	<b>6-41</b>
Transmit Antenna .....	6-41
Spurious Radio Frequency Emissions .....	6-41
Lightning Protection .....	6-42
Rain Proofing .....	6-42
<b>Accessory Installation .....</b>	<b>7-1</b>
<b>TPA 24 Transmit Power Amplifier (Booster).....</b>	<b>7-2</b>
Installing the TPA 24.....	7-3
<b>LNA 10 Low Noise Receive Amplifier .....</b>	<b>7-4</b>
Installing the LNA 10 .....	7-5
<b>RFS 122 Radio Frequency Splitter .....</b>	<b>7-7</b>
Installing the RFS 122 .....	7-7
<b>AL 1 Lightning Arrestor .....</b>	<b>7-8</b>
<b>AMP 2440 Bi-Directional Amplifier .....</b>	<b>7-9</b>
Installing the AMP 2440 Bi-Directional Amplifier.....	7-11
<b>Upgrade Procedure .....</b>	<b>8-1</b>
Maintaining Present Device Settings after Firmware Upgrade .....	8-2
<b>System Troubleshooting.....</b>	<b>9-1</b>
<b>Troubleshooting Guide.....</b>	<b>9-2</b>
<b>Checking Counters .....</b>	<b>9-7</b>
WLAN Counters .....	9-7
Ethernet Counters .....	9-7

<b>Combined Appendices .....</b>	<b>A-1</b>
<b>Supported MIBs and Traps .....</b>	<b>A-2</b>
Supported MIBs .....	A-2
Supported Traps.....	A-22
<b>Technical Specifications .....</b>	<b>A-24</b>
Specifications for BreezeNET PRO.11 Units .....	A-24
Specifications for TPA 24 Transmit Power Amplifier .....	A-28
Specifications for LNA 10 Low Noise Receive Amplifier .....	A-29
Specifications for RFS 122 Radio Frequency Splitter.....	A-30
Specifications for AL 1 Lightning Arrestor .....	A-31
Specifications for AMP 2440 Bi-Directional Power Amplifier.....	A-32
<b>Wireless LAN Concepts.....</b>	<b>A-34</b>
Topology.....	A-35
Roaming.....	A-39
Load Sharing.....	A-40
Dynamic Rate Switching.....	A-41
Media Access .....	A-41
Fragmentation .....	A-41
Collision Avoidance .....	A-42
Channelization .....	A-42
<b>Radio Signal Propagation .....</b>	<b>A-43</b>
RF Terms and Definitions .....	A-44
<b>IEEE 802.11 Technical Tutorial .....</b>	<b>A-53</b>
Architecture Components .....	A-53
IEEE 802.11 Layers Description .....	A-54
The MAC Layer .....	A-55
How Does a Station Join an Existing Cell .....	A-62
Roaming.....	A-63



Keeping Synchronization.....	A-64
Security .....	A-65
Frame Types .....	A-67
Frame Formats .....	A-67
Most Common Frame Formats .....	A-75
Point Coordination Function (PCF) .....	A-77
Ad-Hoc Networks .....	A-78

# Installation Guide



## Table of Figures

Figure 1-1: AP-10 PRO.11 with Two Built-in Omni-Directional Antennas .....	1-6
Figure 1-2: SA-10 PRO.11 with Two Integrated Omni-Directional Antennas.....	1-8
Figure 1-3: SA-40 PRO.11 with Two Integrated Omni-Directional Antennas.....	1-10
Figure 1-4: WB-10D PRO.11 with Two External Antenna Connector Ports .....	1-12
Figure 1-5: SA-PCR PRO.11 PC Card .....	1-14
Figure 2-1: Side Connection Panel.....	2-5
Figure 2-2: Rear Connection Panel .....	2-6
Figure 3-1: Side Connection Panel.....	3-3
Figure 3-2: Main Menu .....	3-12
Figure 3-3: System Configuration Menu .....	3-13
Figure 3-4: Advanced Settings Menu .....	3-24
Figure 3-5: Site Survey Menu .....	3-31
Figure 3-6: Rate Counters .....	3-36
Figure 3-7: Display Rx Packets per Frequency .....	3-37
Figure 3-8: Transmit Statistics .....	3-40
Figure 3-9: Receive Statistics.....	3-41
Figure 3-10: RSSI to dBm Graph.....	3-42
Figure 3-11: Access Control Menu.....	3-44

Figure 4-1: Installing the Windows 2000 Driver Kit .....	4-7
Figure 4-2: System Properties Window – Windows 95B .....	4-12
Figure 4-3: New Hardware Found Window .....	4-13
Figure 4-4: SA-PCR LAN Adapter Properties Window .....	4-15
Figure 4-5: Windows NT Diagnostics Window.....	4-16
Figure 4-6: BreezeCOM SA-PCR Utilities Setup .....	4-22
Figure 4-7: BreezeCOM SA-PCR Utilities - Folder Selection Window .....	4-22
Figure 4-8: BreezeCOM SA-PCR Utilities Setup Complete Window.....	4-23
Figure 4-9: Installing the Windows 2000 Driver Kit .....	4-24
Figure 4-10: SA-PCR Configuration Utility Main Window - Station Status Tab .....	4-28
Figure 4-11: WLAN Parameters Tab .....	4-30
Figure 4-12: Station Control Tab.....	4-32
Figure 4-13: Configuration Access Tab.....	4-33
Figure 4-14: Power Management Tab .....	4-35
Figure 4-15: The Security Tab.....	4-36
Figure 4-16: Maintenance Tab .....	4-38
Figure 4-17: Radio Tab .....	4-40
Figure 4-18: Performance Tab .....	4-41
Figure 4-19: SA-PCR Site Survey.....	4-49
Figure 4-20: Connection Quality Graph .....	4-51
Figure 4-21: Survey Log .....	4-51
Figure 4-22: Upgrade Kit Program Introductory Window .....	4-54
Figure 4-23: Upgrade Kit Program Welcome Window .....	4-55

Figure 4-24: Upgrade Kit Program Step 1 .....	4-55
Figure 4-25: Upgrade Kit Program Step 2 .....	4-56
Figure 4-26: Password Dialog Box .....	4-57
Figure 4-27: Upgrade Program Step 3.....	4-58
Figure 4-28: Upgrade Program Step 4.....	4-58
Figure 4-29: Utilities Directory .....	4-59
Figure 4-30: Upgrade Program Step 5.....	4-59
Figure 5-1: Configuration Utility Window.....	5-3
Figure 5-2: Access Rights Window.....	5-7
Figure 5-3: Secondary Tabs .....	5-9
Figure 5-4: Locate Device Window .....	5-12
Figure 5-5: Set IP Window .....	5-13
Figure 5-6: Device Status Window.....	5-15
Figure 5-7: Send Devices Window.....	5-17
Figure 5-8: Auto-Discovery Settings Window .....	5-19
Figure 5-9: File Menus .....	5-22
Figure 5-10: Create File List Window .....	5-23
Figure 5-11: Mode Menus.....	5-24
Figure 5-12: Tools Menus .....	5-26
Figure 5-13: Multiple Configuration Mode .....	5-29
Figure 5-14: Multiple Configuration Window .....	5-31
Figure 5-15: Firmware Upgrade Window.....	5-33
Figure 5-16: Station Status Tab – Access Point.....	5-38

Figure 5-17: IP Parameters Tab.....	5-40
Figure 5-18: SNMP Parameters Tab.....	5-42
Figure 5-19: WLAN Parameters Tab – Access Point.....	5-44
Figure 5-20: Station Control Tab – Access Point.....	5-48
Figure 5-21: Bridging Tab – Access Point .....	5-50
Figure 5-22: Security Tab.....	5-52
Figure 5-23: Advanced Performance Tab – Access Point .....	5-54
Figure 5-24: Advanced Radio Tab.....	5-56
Figure 5-25: Advanced Access Tab .....	5-57
Figure 5-26: Traffic Counters Tab – Workgroup Bridge.....	5-59
Figure 5-27: Rate Counters Tab – Workgroup Bridge.....	5-61
Figure 5-28: Rate Counters Tab – Access Point .....	5-62
Figure 5-29: Trap Monitor Tab .....	5-64
Figure 6-1: Point-to-Point Configuration/ Connecting Remote Offices to Main Office Network .....	6-4
Figure 6-2: Wireless Bridging Between Two or More Wireless LAN Segments .....	6-6
Figure 6-3: Single Cell Configuration.....	6-7
Figure 6-4: Three Overlapping Cells .....	6-9
Figure 6-5: Multicell Configuration.....	6-11
Figure 6-6: Multi-Hop Configuration .....	6-13
Figure 6-7: Advanced Multihop Configuration .....	6-14
Figure 6-8: BreezeNET LAN in a Typical Office Environment .....	6-15
Figure 7-1: TPA 24 Installation .....	7-3

Figure 7-2: LNA 10 Connections Diagram.....	7-6
Figure 7-3: RFS-122 Connection Diagram .....	7-7
Figure 7-4: AL-1 Connection Block Diagram.....	7-8
Figure 7-5: AMP 2440 Functional Block Diagram .....	7-9
Figure 7-6: AMP 2440 Installation and Mounting .....	7-12
Figure A-1: Wired LAN Topology.....	A-35
Figure A-2: The Basic Wireless LAN Cell .....	A-36
Figure A-3: Wireless LAN Connectivity .....	A-38
Figure A-4: Roaming Through Overlapping Cells.....	A-39
Figure A-5: Common Coverage Area of a Multi-cell Structure .....	A-40
Figure A-6: Typical Radio System.....	A-43
Figure A-7: Attenuation of an RF signal .....	A-44
Figure A-8: Side View.....	A-46
Figure A-9: Top View.....	A-47
Figure A-10: Radiation Pattern of Directional Antenna.....	A-47
Figure A-11: Multipath Reception .....	A-49
Figure A-12: Fresnel Zone.....	A-51
Figure A-13: Fresnel Zone Clear of Obstacles .....	A-51
Figure A-14: Typical 802.11 LAN .....	A-54
Figure A-15: Transaction Between Stations A and B .....	A-58
Figure A-16: Frame Fragmentation .....	A-60
Figure A-17: Access Mechanism.....	A-62
Figure A-18: MAC Frame Format .....	A-68

Figure A-19: Frame Control Field .....	A-69
Figure A-20: RTS Frame Format.....	A-75
Figure A-21: CTS Frame .....	A-76
Figure A-22: ACK Frame Format .....	A-76



# Installation Guide

## Table of Tables

Table 3-1: Hopping Sequences.....	3-17
Table 4-1: SA-PCR Card LED Indications.....	4-20
Table 4-2: Country Domain - Country Code.....	4-71
Table 6-1: Signal Loss Chart.....	6-19
Table 6-2: BreezeNET USA/FCC Range Table - 1Mbps .....	6-27
Table 6-3: BreezeNET USA/FCC Range Table - 2Mbps .....	6-28
Table 6-4: BreezeNET USA/FCC Range Table - 3Mbps .....	6-28
Table 6-5: BreezeNET Europe and ROW Range Table – D Models, DL Models Data Rate = 1Mbps, Sen=-81dBm .....	6-29
Table 6-6: BreezeNET Europe and ROW Range Table – D Models Data Rate = 2Mbps, Sen=-75dBm .....	6-30
Table 6-7: BreezeNET Europe and ROW Range Table – D Models, DL Models Data Rate = 3Mbps, Sen=-67dBm .....	6-30
Table 6-8: BreezeNET Europe and ROW Range Table – DE Models Data Rate = 1Mbps, Sen=-85dBm .....	6-31
Table 6-9: BreezeNET Europe and ROW Range Table – DE Models Data Rate = 2Mbps, Sen=-79dBm .....	6-31
Table 6-10: BreezeNET Europe and ROW Range Table – DE Models Data Rate = 3Mbps, Sen=-71dBm .....	6-31



Table 6-11: BreezeNET Non-Regulation Range Table – D Models Data Rate = 1Mbps, Sen=-81dBm .....	6-32
Table 6-12: BreezeNET Non-Regulation Range Table – D Models Data Rate = 2Mbps, Sen=-75dBm .....	6-32
Table 6-13: BreezeNET Non-Regulation Range Table – D Models Data Rate = 3Mbps, Sen=-67dBm .....	6-33
Table 6-14: TPA-24 and LNA-10 Extension Range Table. Data Rate = 1Mbps, Sen=81dBm .....	6-35
Table 6-15: TPA-24 and LNA-10 Extension Range Table. Data Rate = 2Mbps, Sen=-75dBm .....	6-36
Table 6-16: TPA-24 and LNA-10 Extension Range Table. Data Rate = 3Mbps, Sen=-67dBm .....	6-37
Table 6-17: FCC Available Antennas (USA).....	6-38
Table 6-18: ETSI Available Antennas (Europe and Rest-of-World).....	6-40





# Chapter 1

## Introduction

### About This Chapter

This chapter outlines the scope of this User's Guide, presents the members of the BreezeNET PRO.11 series, describes the benefits of BreezeNET PRO.11 wireless LANs and lists the product specifications.

This chapter is comprised of the following sections:

- ♦ **Scope of the Guide**, page 1-2, provides a descriptive outline of the contents of this User's Guide.
- ♦ **BreezeNET PRO.11 Series Features**, page 1-3, highlights the featured functionality of the BreezeNET PRO.11 series.
- ♦ **BreezeNET PRO.11 Series Product Line**, page 1-5, provides a brief description of the components that comprise the BreezeNET PRO.11 series.
- ♦ **BreezeNET PRO.11 Functional Description**, page 1-16, provides a brief description of the functionality of the BreezeNET PRO.11 system components.

# Scope of the Guide

This User's Guide provides instructions for planning and setting up your wireless LAN, provides details of how to install each unit, and how to install antennas and accessories.

This User's Guide contains the following chapters:

- ◆ **Chapter 1, Introduction:** Describes how to use this guide and presents the components of the BreezeNET PRO.11 series.
- ◆ **Chapter 2, Basic Installation:** Describes how to install BreezeNET PRO.11 series units.
- ◆ **Chapter 3, Device Setup and Management:** Describes how to use the local terminal to setup, configure, and manage BreezeNET PRO.11 series units.
- ◆ **Chapter 4, SA-PCR PRO.11 PC Card Installation, Setup, and Management:** Describes how to install the SA-PCR card, and how to setup and manage the card using the SA-PCR utilities.
- ◆ **Chapter 5, BreezeCONFIG Configuration Utility:** Describes how to use the SNMP Configuration Utility for managing and configuring BreezeNET PRO.11 units.
- ◆ **Chapter 6, Planning and Installing Wireless LANs:** Provides guidelines and restrictions regarding antenna selection and installation, and includes outdoor antenna range tables.
- ◆ **Chapter 7, Accessory Installation:** Introduces some of the accessories available for specific installations, and describes how to install them.
- ◆ **Chapter 8, Upgrade Procedure:** Describes how to perform upgrades for BreezeNET PRO.11 series units using a TFTP application.

- ♦ **Chapter 9, System Troubleshooting:** Contains a troubleshooting guide that provides answers to some of the more common problems that can occur when installing and using BreezeNET PRO.11 series products.
- ♦ **Appendix A, Combined Appendices:** Lists MIBs and traps supported by BreezeNET PRO.11 series products, lists product and attachment specifications, provides an overview of the concepts related to wireless LANs, discusses the concepts and applications of radio signal propagation relevant to wireless LANs, and introduces the new 802.11 standard.

## BreezeNET PRO.11 Series Features

The following comprises the highlights of the BreezeNET PRO.11 series features:

- ♦ **IEEE 802.11 Compliant:** All BreezeNET PRO.11 series units are fully compliant with the final IEEE 802.11 specification for wireless LANs, and thus support interoperability with other IEEE 802.11 compliant vendors.
- ♦ **Fully integrated Product Family:** One high-performance Access Point for all products in the series.
- ♦ **Increased Throughput:** A 3Mbps modem, with up to 2Mbps data throughput.
- ♦ **Translation Bridging:** Support for both translation and transparent bridging as defined in the IEEE 802.1h and RFC 1042 standards.
- ♦ **Seamless Roaming:** Network connection is maintained while roaming between overlapping coverage areas. Transmission and reception can be continued while moving at high speeds with no data packet loss or duplication.
- ♦ **Load Sharing:** Traffic is equally distributed among all Access Points in the area.

- ◆ **Redundancy:** In co-located cell environments, upon failure of an Access Point, stations switch to other available Access Points.
- ◆ **LED Display:** Power, Network Activity, and WLAN Load or Signal Quality LEDs indicate the current status of the unit.
- ◆ **Upgrading:** Simple, quick, and free software upgrades via TFTP.
- ◆ **Future-Proof Investment:** All items in the PRO.11 Series line can be freely and quickly upgraded with flash updates.
- ◆ **SA-PCR Card:** The SA-PCR PRO.11 PC card is extremely compact and does not extend beyond your PC. It comes with two retractable antennas, or two connectors to which antennas may be connected. Multi-rate support for 1, 2, and 3Mbps guarantees efficient use of the medium. Throughput is up to 2Mbps: the highest rate on the market!
- ◆ **Configuration Utility:** This user-friendly application helps you quickly setup stations containing the SA-PCR card. You can save the configuration to a file and import the file to other stations for fast installation.
- ◆ **Site Survey Utility:** This user-friendly application records the signal strength received by the SA-PCR Card at different locations, giving a clear image of existing coverage. The gathered data indicates whether to add, remove, or move Access Points.

# BreezeNET PRO.11 Series Product Line

The BreezeNET PRO.11 series product line consists of the following components:

Product Name	Available Types	Antenna Type
Access Point	AP-10 PRO.11 AP-10D PRO.11 AP-10DL PRO.11	Internal External External
Single Station Adapter	SA-10 PRO.11 SA-10D PRO.11 SA-10DL PRO.11	Internal External External
Four Port Station Adapter	SA-40 PRO.11 SA-40D PRO.11 SA-40DL PRO.11	Internal External External
Workgroup Bridge	WB-10 PRO.11 WB-10D PRO.11 WB-10DL PRO.11	Internal External External
PCMCIA PC Card Station Adapter Card	SA-PCR PRO.11 SA-PCD PRO.11	Internal External
Extended Range Access Point	AP-10DE	External
Extended Range Bridge	WB-10DE	External

**NOTES:**

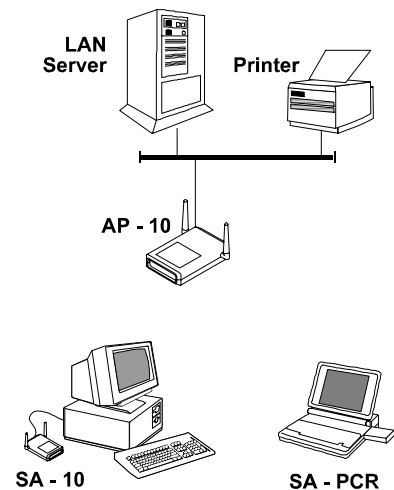
The WB-10DE and AP-10DE are not compatible with the BreezeNET PRO.11 series. Units in the BreezeNET PRO.11 series are not compatible with units in the BreezeNET PRO series.

## BreezeNET PRO.11 Access Point

The BreezeNET PRO.11 Access Point is fully compliant with the IEEE 802.11 Wireless LAN standard.

The Access Point is a wireless hub that provides access for wireless workstations into wired Ethernet LANs. It also contains the wireless relaying function that enables workstations equipped with a Station Adapter (Station Adapter, Bridge, and SA-PCR) to communicate with one another inside the cell coverage area (even if they are not in direct line of sight) via the Access Point. Any two wireless stations in two different cells can communicate through their Access Points.

The BreezeNET Access Point can support various data rates simultaneously at 3Mbps, 2Mbps or 1Mbps.



**Figure 1-1: AP-10 PRO.11 with Two Built-in Omni-Directional Antennas**



Mobile workstations, such as laptops and hand-held devices, can roam between Access Points that belong to the same Extended Service Set (ESS). In an Extended Service Set, all Access Points have the same ESSID. When the access points are set up so that their coverage areas overlap, users can roam seamlessly from cell to cell. This means that there is no network connection interruption when moving from one coverage area to the other through the overlap area. The roaming is completely transparent to the user and the applications. The Station Adapters decide when a mobile user becomes disassociated from one Access Point and associated with another. This process is fully transparent, requires no user intervention and involves no loss of data packets.

Multiple Access Points can be positioned in locations where heavy network traffic is expected; this creates a multicell and increases the aggregate throughput capacity in areas where it is needed most. The system implements a Load Balancing algorithm to divide the stations equally between the available co-located Access Points.

The Access Point contains an embedded SNMP agent, enabling effective management by BreezeVIEW or any standard SNMP management station. Software upgrades can be downloaded by TFTP protocol via the wired LAN or wireless LAN.

The Access Point is available in three models:

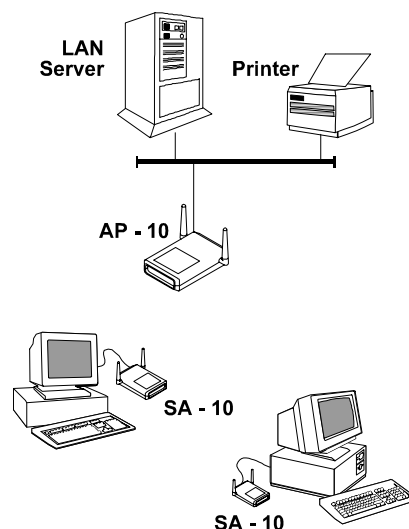
- ◆ AP-10 PRO.11 with two integrated omni-directional antennas.
- ◆ AP-10D PRO.11 for use with external high-gain antenna(s).
- ◆ AP-10DL PRO.11 for use in Europe with high-gain antenna under the ETSI standard.

## BreezeNET PRO.11 Single Station Adapter

The BreezeNET PRO.11 Single Station Adapter is a wireless LAN station adapter that converts any device equipped with an Ethernet interface into a wireless LAN station. The Single Station Adapter is transparent to the device's hardware, software, and network operating system. This enables plug-and-play installation.



**Figure 1-2: SA-10 PRO.11 with Two Integrated Omni-Directional Antennas**



The Single Station Adapter enables its workstation to communicate with any other wireless station in the same cell coverage area, and to access all network resources such as file servers, wired stations, printers and shared databases via the Access Point. Any two wireless stations in two different cells can communicate through their Access Points.

Workstations that can be connected to the wireless LAN include PCs, X-Terminals, and any other device that supports Ethernet. The unit is transparent to the workgroup devices' hardware, software, and network operating system.

The Single Station Adapter contains an embedded SNMP agent that enables effective management. Software upgrades are downloaded by TFTP via the Ethernet port or via the wireless LAN and Access Point.

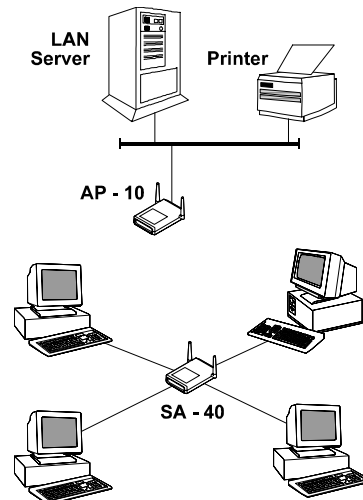
Network connection is maintained while roaming between overlapping coverage areas. Transmission and reception can be continued while moving at high speed with no data packet loss or duplication.

The Single Station Adapter is available in three models:

- ◆ SA-10 PRO.11 with two integrated 2dbi omni-directional antennas.
- ◆ SA-10D PRO.11 for use with external antenna(s).
- ◆ SA-10DL PRO.11 for use in Europe with high-gain antenna under the ETSI standard.

## BreezeNET PRO.11 Four Port Station Adapter

The BreezeNET PRO.11 Four-Port Workgroup Adapter is a wireless LAN adapter that connects a workgroup of up to four Ethernet-equipped workstations to the wireless LAN. The Four Port Station Adapter is transparent to the workgroup devices' hardware and software, enabling plug-and-play installation.



**Figure 1-3: SA-40 PRO.11 with Two Integrated Omni-Directional Antennas**

The Four Port Station Adapter enables connected workstations to communicate with other wireless stations in the same cell coverage area, and to access all network resources such as file servers, wired stations, printers and shared databases via the Access Point. The Four Port Station Adapter also allows highly efficient and fast wired communication among the four connected workstations.

Workstations that can be connected to the wireless LAN include PCs, X-Terminals and any other device that supports Ethernet. The unit is transparent to the workgroup devices' hardware, software, and network operating system.

The BreezeNET Four Port Station Adapter contains an embedded SNMP agent and software downloading capabilities which enabled it to be effectively managed. Software upgrades are downloaded by TFTP protocol via the Ethernet ports or via the Wireless LAN and Access Point.

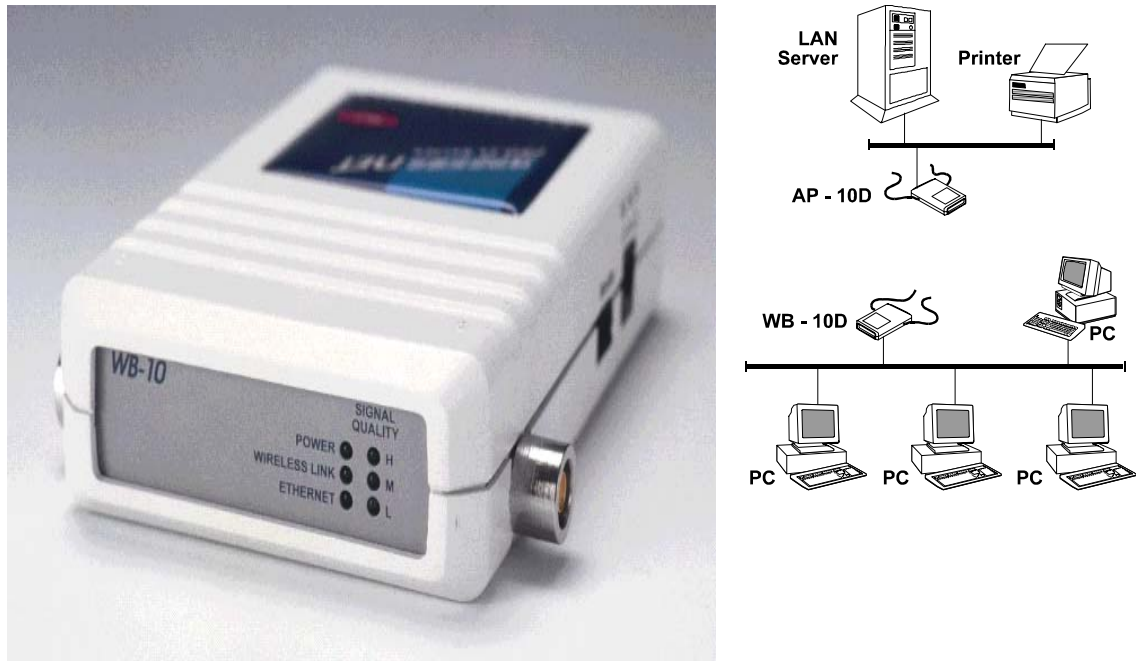
Network connection is maintained while roaming between overlapping coverage areas. Transmission and reception can be continued while moving at high speed with no data packet loss or duplication.

The Four Port Station Adapter is available in three models:

- ◆ SA-40 PRO.11 with two integrated omni-directional antennas.
- ◆ SA-40D PRO.11 for use with external antenna(s).
- ◆ SA-40DL PRO.11 for use in Europe with high-gain antenna under the ETSI standard.

## BreezeNET PRO.11 Workgroup Bridge

The BreezeNET Workgroup Bridge is a high-speed, wide-range wireless LAN bridge that provides connectivity to remote Ethernet networks.



**Figure 1-4: WB-10D PRO.11 with Two External Antenna Connector Ports**

The Workgroup Bridge communicates with the Access Points of the remote LANs, effectively creating an extended wireless network spanning sites situated up to 6 miles apart (in Europe, this range is limited by ETSI regulations to 2.5 Km; in deregulated regions, this range can be up to 60 Km). In this way, a central Ethernet LAN may be connected with one or more branch office LANs.

In addition, an island consisting of a Workgroup Bridge together with an Access Point can work as a relay. Transmissions from the central and remote LAN relayed via the island located between them. This configuration effectively doubles the bridge range.

Workstations that can be connected to the wireless LAN include PCs, X-Terminals and any other device that supports Ethernet. The unit is transparent to the workgroup devices' hardware, software, and network operating system.

The BreezeNET Workgroup Bridge contains an embedded SNMP agent and software downloading capabilities enabling effective management. Software upgrades are downloaded using TFTP protocol via the Ethernet ports or via the wireless LAN and Access Point.

The Workgroup Bridge is available in three models:

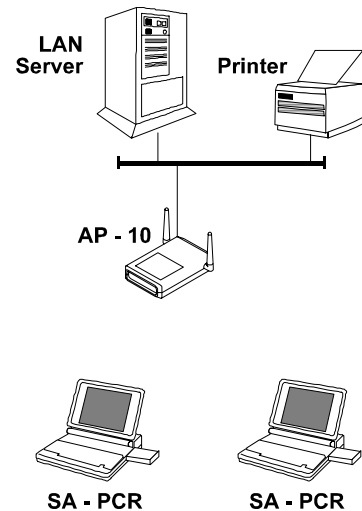
- ◆ WB-10 PRO.11 with two integrated 2dbi omni-directional antennas.
- ◆ WB-10D PRO.11 with two external antenna connector ports.
- ◆ WB-10DL PRO.11 for use in Europe with high gain antenna under the ETSI standard.

## BreezeNET PRO.11 SA-PCR Card

The PC Card provides the portable computer user with continuous connectivity and complete mobility, enabling seamless roaming throughout the wireless LAN campus.



**Figure 1-5: SA-PCR PRO.11 PC Card**



The BreezeNET PRO.11 SA-PCR card converts any portable computer (including notebooks, laptops, pen-based and handheld computers) containing a PCMCIA Release 2.1 type II slot into a wireless LAN workstation.

The SA-PCR card can communicate with any other wireless station in its cell coverage area. Furthermore, any two wireless stations in two different cells can communicate through their Access Points. The SA-PCR card can access all network resources such as file servers, other wired stations, printers and shared databases via the BreezeNET Access Point.

Network connection is maintained while roaming between overlapping cell coverage areas. Transmission and reception can be continued while moving at high speed with no data packet loss or duplication.



The SA-PCR Card is available in two models:

- ◆ SA-PCR PRO.11 with two integrated omni-directional retractable antennas.
- ◆ SA-PCD PRO.11 with two external antenna connector ports.

## BreezeNET PRO.11 Extended Range Access Point and Bridge

**NOTE:**

This product complies with European ETSI 300-328 and should only be used in countries that implement this standard.

The BreezeNET PRO.11 WB-10DE is a high-speed, wide-range wireless LAN bridge that provides connectivity to remote Ethernet networks.

The WB-10DE communicates with the BreezeNET AP-10DE Access Points of the remote LANs, effectively creating an extended wireless network spanning sites situated up to 5Km apart. In this manner, a central Ethernet LAN may be connected with one or more branch office LANs.

The WB-10DE and AP-10DE products comply with European ETSI standard 300-328. They should not be used in countries where FCC standards are applicable.

The WB-10DE and AP-10DE can be used as a point-to-point or a point-to-multipoint solution.

**NOTE:**

The WB-10DE and AP-10DE are not compatible with the BreezeNET PRO.11 series. The SA-10 PRO.11, SA-PCR PRO.11, SA-40 PRO.11, AP-10 PRO.11 and WB-10 PRO.11 units cannot communicate with the AP-10DE or the WB-10DE.

The BreezeNET AP-10DE and WB-10 DE contain an embedded SNMP agent and software downloading capabilities enabling effective management. Software upgrades are downloaded using TFTP protocol via the Ethernet ports or via the wireless LAN and Access Point.

The BreezeNET DE Access Point and Bridge are available for use with external antenna connector ports.

## **BreezeNET PRO.11 Functional Description**

BreezeNET PRO.11 units add wireless functionality to existing Ethernet LANs.

### **Quick Review of Ethernet**

Standard Ethernet LAN stations are wired to a common bus. When one of the stations sends a message, it assigns a destination address to the message and sends the message on the bus. All stations on the bus “hear” the message, but only the station with the matching address processes the message.

### **Startup Procedure**

When wireless units (other than the AP-10) start up, they scan the frequencies for an AP-10. If an active AP-10 is in range, the units synchronize with it. The addresses associated with the units are registered in the AP-10 (the registration process is different for each unit type). From then on, the units can send and receive messages to and from the wired LAN.

## **AP-10 Access Point**

The AP-10 Access Point is connected to a wired Ethernet LAN and keeps a list of known stations on its wireless side. When an AP-10 “hears” a message that is destined for a wireless station, the AP-10 forwards the message wirelessly to the station. If the message has a destination address that the AP-10 does not recognize, the AP-10 ignores the message.

In addition, the AP-10 continuously “listens” for wireless messages. When the AP-10 “hears” a wireless message destined for another wireless unit, it relays the message directly to the wireless unit without forwarding the message to the wired LAN. When the AP-10 “hears” a wireless message the destination of which is not on the wireless LAN, it forwards the message to the wired LAN. Messages cannot be sent directly between wireless stations without an AP-10 to relay the message.

## **SA-10 Station Adapter**

The SA-10 Station Adapter is connected to a station’s network card. When the station sends a message, the SA-10 wirelessly forwards it to the AP-10. And when the AP-10 receives a message destined for the station, it wirelessly forwards the message to the SA-10.

The first time the station sends a message, the station’s address is registered in the AP-10. The AP-10 keeps only the first address for each SA-10, so the SA-10 will not work properly if connected to more than one station.

## **SA-40 Station Adapter**

The SA-40 Station Adapter has four connectors for up to four stations, and features operation identical to that of the SA-10. As each station connected to the SA-40 sends its first message, each address is registered in the AP-10. The AP-10 keeps up to four addresses for each SA-40, so the SA-40 will not operate properly if connected to more than four stations.

## **WB-10 Wireless Bridge**

In contrast to the SA-10 and SA-40 that connect directly to stations, the WB-10 Wireless Bridge connects to a wired Ethernet LAN (hub). When a station on the WB-10's LAN sends a message that is not destined for a local station, the WB-10 wirelessly forwards the message to the AP-10. When the AP-10 receives a message destined for a station on the WB-10's LAN, the AP-10 wirelessly forwards it to the WB-10. In this way, the WB-10 and AP-10 work together like a standard network bridge.

The first time each station on the WB-10's LAN sends a message, the station's address is registered in the WB-10 and the AP-10. The WB-10 and AP-10 can hold all the addresses necessary to support an entire LAN connected to a WB-10.

## **SA-PCR Station Adapter**

The SA-PCR station adapter is inserted into the station's PCMCIA slot and features identical operation to that of the SA-10. In contrast to the SA-10 and SA-40 station adapters that connect to the station's network card, the SA-PCR is the station's network card. The SA-10 and SA-40 can be used with stations of any operating system as long as the station sends legal Ethernet messages. The SA-PCR requires a driver that is compatible with the station's operating system.







# Chapter 2

## Basic Installation

### About This Chapter

This chapter describes the physical installation of the BreezeNET PRO.11 series units described in Chapter 1, with the exception of the SA-PCR card. Installation of the SA-PCR PRO.11 PC card is described in Chapter 4.

The BreezeNET PRO.11 series features plug-and-play operation, i.e., the unit starts operating immediately after physical installation with a set of default operation parameters. A local terminal can be connected to the unit to perform system-specific parameter setting. The use of a local terminal and the configuration parameters are described in Chapter 3. In addition, all products in the PRO.11 series contain an SNMP agent and can be configured from a remote location via the network. This is described in the Appendix.

This chapter is comprised of the following sections:

- ◆ **Basic Installation Checklist**, page 2-2, outlines the steps required for installation.
- ◆ **Checking the Packing List**, page 2-2, provides a list of the contents of the installation kit.
- ◆ **Positioning the Unit**, page 2-3, provides guidelines for positioning the units for optimal transmission and reception.

- ◆ **Connecting the Unit to the Power Supply**, page 2-5, describes how to attach the unit to its power source.
- ◆ **Connecting the Unit to the Ethernet Port**, page 2-6, describes how to connect the unit to the Ethernet, ensuring functional connectivity.
- ◆ **Checking Unit Functionality**, page 2-7, describes how to ensure that the unit is functioning properly.

## Basic Installation Checklist

Standard installation involves the following steps:

- ◆ Checking the packing list
- ◆ Positioning the unit and the antenna in the best location
- ◆ Connecting the power supply to the unit
- ◆ Connecting the Ethernet port to the unit
- ◆ Checking unit functionality using the LED indicators

## Checking the Packing List

To ensure efficient installation, first verify that the unit is complete with the following components:

- ◆ The unit, complete with two omni-directional antennas or RF connectors for use with external antennas (D models).
- ◆ Quick Installation Guide/Card.
- ◆ 5V DC power supply transformer.
- ◆ Mounting bracket for wall or ceiling installations and torque key for antenna connectors (supplied with D models).



- ◆ The AP-10 PRO.11 and AP-10DE Access Points come with the following additional components:
  - ❖ The *BreezeNET PRO.11 Series User's Guide*.
  - ❖ A monitor connector cable for connecting the units to a monitor in order to perform Local Terminal Management functions.
  - ❖ Proprietary MIB disk for performing remote unit configuration and monitoring via SNMP (see the Appendix).

Open the packaging carefully and make sure that none of the items listed above are missing. Do not discard packaging materials. If, for any reason, the unit is returned, it must be shipped in its original package.

## Positioning the Unit

BreezeNET PRO.11 wireless LAN products are robust, trouble-free units, designed to operate efficiently under a wide range of conditions. The following guidelines are provided to help you position the units to ensure optimum coverage and operation of the wireless LAN.

### Metal Furniture

Position the units clear of metal furniture and away from moving objects such as metal fans or doors.

### Microwave Ovens

For best performance, position the units clear of radiation sources that emit in the 2.4 GHz frequency band, such as microwave ovens.

## Antennas

For models with integrated antennas, make sure the antennas are extended upward vertically in relation to the floor. For models with external antennas, connect the external antennas and RF cable. For information regarding external antenna installation, refer to *Outdoor Installation Considerations*, on page 6-21.

## Heat Sources

Keep the units well away from sources of heat, such as radiators and air conditioners.

## Additional Considerations When Positioning the Access Point

When positioning the AP-10 PRO.11 and AP-10DE Access Points, take into account the following additional considerations.

### Height

Install the Access Point at least 1.5m above the floor, clear of any high office partitions or tall pieces of furniture in the coverage area. The Access Point can be placed on a high shelf, or can be attached to the ceiling or a wall using a mounting bracket.

## Central Location

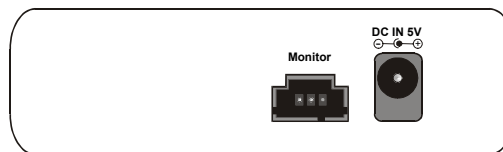
Install the Access Point in a central location in the intended coverage area. Optimal positions include:

- ♦ In the center of a large room
- ♦ In the center of a corridor
- ♦ At the intersection of two corridors

Many modern buildings have partitions constructed of metal or containing metal components. We recommend that you install the Access Points on the corridor ceilings. The radio waves propagated by the BreezeNET PRO.11 LAN are reflected along the metal partitions and enter the offices through the doors or glass sections.

## Connecting the Unit to the Power Supply

The unit operates on a power input of 5VDC, (1200mA, 1500mA peak) supplied by the power transformer included with the unit.



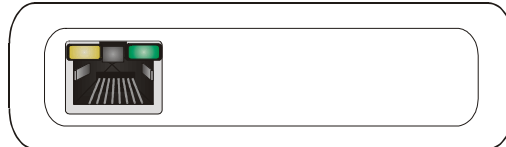
**Figure 2-1: Side Connection Panel**

- 1.** Plug the output jack of the power transformer into the DC input socket on the side panel of the unit.
- 2.** Connect the supplied power transformer to a power outlet - 110/220 VAC.

# Connecting the Unit to the Ethernet Port

This section describes how to connect the units to the Ethernet port.

1. Connect one end of an Ethernet 10BaseT cable (not supplied) to the RJ-45 port on the rear panel of the unit (marked UTP).



**Figure 2-2: Rear Connection Panel**

2. Connect the other end of the connector cable to the Ethernet outlet:
  - ◆ When connecting an SA-10 or SA-40 to a PC, use a straight cable.
  - ◆ When connecting an AP-10 or WB-10 to a LAN, use a straight cable.
  - ◆ When connecting an AP-10 or WB-10 to a PC, use a crossed cable.
  - ◆ When connecting an AP-10 to a WB-10, use a crossed cable.

# Checking Unit Functionality

Verify that the unit is functioning correctly via the front panel LEDs. The following tables describe the front panel LEDs for stations (SA-10, SA-40) and bridges (WB-10), and for Access Points.

## Station (SA-10, SA-40) and Bridge (WB-10) LEDs

Name	Description	Functionality
PWR	Power supply	On – After successful power up Off – Power off
WLNK	WLAN Link	On – Unit is synchronized or associated with an AP Off – Unit is not synchronized or associated with an AP
ETHR	Ethernet activity	On – Reception on Ethernet port Off – No reception on Ethernet port
QLT	Quality of reception	<p>QLT ○ H very low quality reception or not synchronized with Access Point ○ M less than -81 dBm ○ L</p> <p>QLT ○ H low quality reception (usually enabling 1 Mbps traffic) ○ M from -81 to -77 dBm ● L</p> <p>QLT ○ H medium quality reception (usually enabling 2 Mbps traffic) ● M from -77 to -65 dBm ● L</p> <p>QLT ● H high quality reception (usually enabling 3 Mbps traffic) ● M greater than -65 dBm ● L</p>

## Access Point LEDs

Name	Description	Functionality
PWR	power supply	On – After successful power up Off – Power off
INFR	radio interference	Off – No interference Blinking – Interference present
ETHR	Ethernet activity	On – Reception of data from Ethernet LAN that is forwarded to WLAN (in reject unknown mode)  Off – No reception of data from Ethernet LAN that is forwarded to WLAN
LOAD	WLAN load Number of associated stations	<div> LOAD  ○ H  ○ M  ○ L  no stations </div> <div> LOAD  ○ H  ○ M  ● L  1-8 stations </div> <div> LOAD  ○ H  ● M  ● L  9-16 stations </div> <div> LOAD  ● H  ● M  ● L  17 or more stations </div>

## **Verifying the Ethernet Connection**

Once you have connected the unit to an Ethernet outlet, verify that the ETHR LED on the front panel is blinking. The ETHR LED should blink whenever the unit receives LAN traffic.

At the other end of the Ethernet link, verify that the LINK indicator is ON. On APs, the LINK indicator is located on the attached hub port; on Station Adapters, the LINK indicator is located on the NIC.







# Chapter 3

## Using the Local Terminal for Unit Setup and Management

### About This Chapter

BreezeNET PRO.11 series units feature plug-and-play operation; the unit starts operating immediately following physical installation with a set of default parameters. System-specific configuration of the unit to meet specific requirements can be accomplished via a local terminal (ASCII ANSI terminal or PC) connected to the unit.

This chapter describes how to use the local terminal to configure and manage the BreezeNET PRO.11 series units described in Chapter 1, with the exception of the SA-PCR card. Configuration and management of the SA-PCR card is described in Chapter 4.

This chapter is comprised of the following sections:

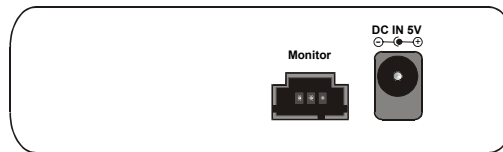
- ◆ **Getting Started with the Local Terminal**, page 3-3, describes how to set up and work with the local terminal.
- ◆ **Configuration Screens**, page 3-4, describes how to access and navigate the configuration screens.

- ◆ **Main Menu**, page 3-12, describes the menu available through the *Main* menu.
- ◆ **System Configuration Menu**, page 3-13, describes the menu and parameters available through the *System Configuration* menu.
- ◆ **Advanced Settings Menu**, page 3-24, describes the menus and parameters available through the *Advanced Settings* menu.
- ◆ **Site Survey Menu**, page 3-31, describes how to operate the Site Survey software and describes the statistics available through the *Site Survey* menu.
- ◆ **Access Control Menu**, page 3-44, describes how to limit access to the unit for configuration and management purposes.
- ◆ **Code Activate Control Menu**, page 3-46, describes the functionality available through the *Code Activate Control* menu.

# Getting Started with the Local Terminal

This section describes how to set up the local terminal utility.

1. Use the Monitor cable supplied with the Access Point. Connect one end of the cable to the MON jack on the side panel of the unit and the other end to the COM port of the terminal.



**Figure 3-1: Side Connection Panel**

2. Run a terminal emulation program (such as HyperTerminal).
3. Set the communication parameters to the following:

Baud Rate:	9600
Data Bits:	8
Stop Bits:	1
Parity:	None
Flow Control:	None
Connector:	Connected COM port.
4. Click **Enter**. The *Main* menu is displayed.

➤ **To use Local Terminal Management:**

- 1.** Click an option number to open/activate the option. You may need to press **Enter** in some cases.
- 2.** Press **Esc** to exit a menu or option.
- 3.** Reset the unit after making configuration changes.

## Configuration Screens

Listed below are the menus, sub-menus, and parameters/options in the terminal program that can be edited by an Installer user. Default values are listed where applicable.

Numbers in the table below indicate how to reach each option. For example, to reach the 1.2.1 **IP Address** option, start at the *Main* menu and press **1**, then **2**, and then **1**.

Menu	Sub-Menu	Sub-Menu	Default Values
1. System Configuration	1.1. Station Status		
	1.2. IP and SNMP Parameters	1.2.1 IP Address 1.2.2 Subnet Mask 1.2.3 Default Gateway Address 1.2.4 SNMP Traps 1.2.5 DHCP Client 1.2.S Display Current Values	Enabled    Disabled

Menu	Sub-Menu	Sub-Menu	Default Values
	1.3. Wireless LAN (WLAN) Parameters	1.3.1 Hopping Sequence (only for AP) 1.3.2 Hopping Set (only for AP) 1.3.3 ESSID 1.3.4 Max. Data Rate 1.3.5 Transmit Antenna 1.3.6 Mobility 1.3.7 Load Sharing 1.3.8 Preferred AP (not available for APs) 1.3.9 Use Prefix ESSID (For AP only) 1.3.A Prefix ESSID (For AP only) 1.3.B Station Mode (For SA only) 1.3.S Display Current Values	1 1 ESSID1 3Mbps Use 2 Antennas Low Disabled Not Set Disabled ESSID1 Access Station
	1.4. Bridging	1.4.1 LAN to WLAN Bridging Mode (AP only) 1.4.2 Intelligent Bridging Period (AP only) 1.4.3 IP Filtering 1.4.4 Tunneling 1.4.5 Broadcast Relaying 1.4.6 Unicast Relaying 1.4.7 Association Aging Period	Reject Unknown 15 sec Disabled Both Enabled Enabled Enabled Disabled

Menu	Sub-Menu	Sub-Menu	Default Values
	1.5. Station Control	1.5.1 Reset Unit 1.5.2 Load Defaults	
	1.6. Security	1.6.1 Authentication Algorithm 1.6.2 Default Key ID 1.6.3 Pre-authentication 1.6.4 Authentication Option Installation 1.6.A WEP Key #1 1.6.B WEP Key #2 1.6.C WEP Key #3 1.6.D WEP Key #4 1.6.S Display Keys	Open system 1 Disabled Privacy option not implemented 0000000000 0000000000 0000000000 0000000000
2. Advanced Settings	2.1. Translation Mode		Enabled

Menu	Sub-Menu	Sub-Menu	Default Values
	2.2 Roaming	2.2.1 Max. Number of Scanning 2.2.2 Roaming Decision Window 2.2.3 Roaming Decision Numerator 2.2.4 Roaming Decision RSSI Threshold 2.2.5 Joining Decision RSSI Threshold 2.2.6 Number of Beacons for Disconnect Reasons 2.2.7 Number of Probe Responses 2.2.8 Neighboring Beacon Rate	70 10 6 60 70 6 1 40
	2.3. Performance	2.3.1 Dwell Time 2.3.2 RTS Threshold 2.3.3 Max. Multicast Rate 2.3.4 Power Save Support 2.3.5 DTIM Period 2.3.6 IP Stack 2.3.7 Acknowledge Delay 2.3.8 Beacon Interval 2.3.9 Contention Window 2.3.10 Associate with AP running S/W Version 4.X and below	128 120 bytes 1 Mbps Disabled 4 Enabled Regular 2 dwells 7 Disabled

Menu	Sub-Menu	Sub-Menu	Default Values
	2.4. Radio	2.5.1 Hopping Standard 2.5.2 Display Site Proprietary Sequences 2.5.3 Power level 2.5.4 Carrier sense level 2.5.5 Carrier Sense Difference level 2.5.6 Noise Floor 2.5.7 External Amplifier	US FCC  High 48 10 -92dbm Disabled
	2.5. Rate	2.5.1 Multi-Rate Support 2.5.2 Multi-Rate Decision Window Size	Enabled 3
	2.6. AP Redundancy Support		Disabled
	2.7. Maintenance	2.7.1 Wait for Association Address 2.7.2 Japan Call Sign	Wait for update via Ethernet



Menu	Sub-Menu	Sub-Menu	Default Values
	2.8 Voice and Data Configuration	2.8.1 Enable Voice 2.8.2 Max. Number of Retransmissions in Voice Packets 2.8.3 Number of Dwells to Retransmit in Voice Packets 2.8.5 Max. Number of Dwells to Retransmit in Data Packets 2.8.6 Number of Dwells to Retransmit in Data Packets 2.8.S Display Current Values	Voice disabled 3 0 1 2
	2.9 AP Redundancy Support Limit		10
3. Site Survey	3.1. System Counters	3.1.1 Display Ethernet and WLAN Counters 3.1.2 Display Rate Counters 3.1.3 Display Rx packets per frequency 3.1.4 Reset All Counters 3.1.5 Power Saving Counters 3.1.6 Display Quality Counters	
	3.2 Survey Software		

Menu	Sub-Menu	Sub-Menu	Default Values
	3.3. Event Log	3.3.1 Display Event Log 3.3.2 Erase Event Log 3.3.3 Event display policy	Show Informational severity and higher
	3.4. Display Neighboring APs		
4. Access Control	4.1. Change Access Rights	4.1.0 User 4.1.1 Installer 4.1.2 Technician	Installer
	4.2. Change Installer Password		"inst2000"
	4.3. Change Write Community Password		"private"
	4.4. Change Read Community Password		"public"
	4.S Display Current Values		
5. Code Activate Control	5.1. Try To Run From Non-Active Code		
	5.2. Check Non-Active Code State		

\* Option 1.3.5 Transmit Antenna has the default value Use #2 for the SA-40 unit only.

\*\* Option 1.3.7 Load Sharing has the default value Enabled for the AP-10 unit only.

## Main Menu

The *Main* menu of the Local Terminal management application provides access to all required configuration screens, as shown below.

```
BreezeNET PRO.11 Series (AP-10 DL)
Version : 5.10
Tue Oct 17 12:58:47 2000
BreezeNET Monitor
=====
1 - System Configuration
2 - Advanced Settings
3 - Site Survey
4 - Access Control
5 - Code Activate Control
Select option >
```

**Figure 3-2: Main Menu**

# System Configuration Menu

The *System Configuration* menu provides access to the most commonly required configuration screens.

```
BreezeNET PRO.11 Series (AP-10 DL)
Version : 5.10
Tue Oct 17 12:58:47 2000
BreezeNET Monitor
=====
1 - Station Status
2 - IP and SNMP Parameters
3 - Wireless LAN Parameters
4 - Bridging
5 - Station Control
6 - Security
Select option >
```

**Figure 3-3: System Configuration Menu**

## Station Status

*Station Status* is a read-only sub-menu that displays the current values of the following parameters:

- ◆ **Unit's Mode:** Identifies the unit's function. For example, if the unit is an Access Point, **AP-10** appears in this field. If the unit is a Station Adapter i.e., SA-10, SA-40 or a WB-10, SA-10, SA-40 or **WB-10** appears in this field.
- ◆ **Unit's HW Address:** Displays the unit's unique MAC address.

- ◆ **Unit's WLAN Address (SA or WB):** The address associated with the unit. For an SA-10 configured to Access Station mode, this is the MAC address of the unit. For an SA-10 configured to use the host MAC address for association, this is the address of the host. For the SA-40 and WB-10, this is the MAC address of the unit. This field does not appear when the unit is an AP.
- ◆ **Station Status (SA or WB):** Current status of the station. This field does not appear when the unit is an AP. There are three possible display options:
  - ❖ **Scanning:** The station is searching for an AP with which to associate.
  - ❖ **Sync Waiting for Address:** The station is synchronized with an AP but has not yet learned its WLAN MAC address (this option is relevant only to the SA-10). The AP does not forward packets to the station when it is in this mode.
  - ❖ **Associated:** The station is associated with an AP and has adopted the attached PC MAC address (for SA-10 units configured to use the host MAC address for association) or uses the unit's hardware address (SA-40, WB-10 and SA-10 units configured to Access Station mode), and is receiving packets from the LAN.
- ◆ **AP Address (Station Only):** For stations, this parameter indicates an address of the AP with which the unit is currently associated.
- ◆ **Total Number of Associations since last reset (Station Only):** For stations, this indicates the total number of associations and disassociations with various APs. This is usually an indication of roaming.
- ◆ **Current Number of Associations (AP Only):** Total number of stations currently associated with an AP.

- ◆ **Maximum number of Associations since last reset (AP Only):**  
Maximum number of stations that were associated with an AP since the last reset.
- ◆ **Current Number of Authentications (AP Only):** Total number of stations currently authenticated with an AP. A station may be concurrently authenticated with several APs, but is associated with only one AP at a time.
- ◆ **Maximum number of Authentications since last reset (AP Only):**  
Maximum number of stations that were authenticated with an AP since the last reset.

## IP and SNMP Parameters

All BreezeNET PRO.11 units contain IP host software. This software can be used for testing the unit for SNMP management functions and for downloading software upgrades using the TFTP protocol.

- ◆ **IP Address:** IP address of the unit.
- ◆ **Subnet Mask:** Subnet mask of the unit.
- ◆ **Default Gateway Address:** Gateway address of the unit.
- ◆ **SNMP Traps:** Type **0** to disable SNMP trap sending.  
Type **1** to enable SNMP trap sending. When an event occurs, a trap is sent to the defined host address (see the Appendix for a list of traps). You can configure the host address to which the traps are sent via the SNMP management application.

- ◆ **DHCP Client:** Defines the DHCP mode. Available selections include:
  - ❖ **Disabled:** IP Address configuration is always manual.
  - ❖ **DHCP Only:** The IP Address configuration is always automatic, using a DHCP server.
  - ❖ **Automatic:** If a DHCP Server was found (within 4 minutes), then the IP address configuration is accomplished using the DHCP Server; otherwise, the IP address configuration is manual.
- ◆ **Display Current Values:** Type S to displays information concerning the current status of all IP-related parameters.

## Wireless LAN (WLAN) Parameters

The *WLAN Parameters* menu contains the following options:

- ◆ **Hopping Sequence (AP Only):** Hopping sequence of the unit. A hopping sequence is a pre-defined series of channels (frequencies) that are used in a specific, pseudo-random order as defined in the sequence. The unit “hops” from frequency to frequency according to the selected sequence. When more than one AP is co-located in the same area (even if they are not part of the same network) it is recommended to assign a different hopping sequence to each AP.

Hopping sequences are grouped in three hopping sets (described in the following parameter). When setting up multiple APs in the same site, always choose hopping sequences from the same hopping set. This reduces the possibility of collisions on the WLAN.

This parameter is set only for the BreezeNET PRO.11 Access Point. It is not accessible from any other BreezeNET PRO.11 unit. During the association process, all other stations learn the hopping sequence from the Access Point. Different co-located WLAN segments should use different hopping sequences.



- ◆ **Hopping Set (AP Only):** Hopping set (between **1** and **3**) of the unit. Hopping sequences are grouped in several hopping sets. Always use the same hopping set per site.

The number of hopping sequences per set is different for each hopping standard according to the following table:

**Table 3-1: Hopping Sequences**

Hopping Standard	Number of Sequences per Hopping Set
Australia	20
Canada	10
Europe ETSI	26
France	11
Israel	11
Japan	4
Korea	4
Netherlands	5
Singapore	12
Spain	9
US FCC	26

- ◆ **ESSID:** The ESSID (up to 32 printable ASCII characters) of the unit is a string used to identify a WLAN. This ID prevents the unintentional merging of two co-located WLANs. A station can only associate with an AP that has the same ESSID. Use different ESSIDs to segment the WLAN network and add security.

**NOTE:**

The ESSID parameter is case-sensitive.

- ◆ **Maximum Data Rate:** Maximum data rate of the unit. BreezeNET PRO.11 units operate at 1Mbps, 2Mbps or 3 bps. The unit adaptively selects the highest possible rate for transmission. Under certain conditions (compatibility reasons or for range/speed trade-off) you may decide to limit the use of higher rates.
- ◆ **Transmit Antenna (also referred to as Transmit Diversity):** The selection of antennas used for transmission. During reception, a BreezeNET PRO.11 unit dynamically selects the antenna where reception is optimal. In contrast, the unit selects the antenna from which it will transmit before transmission. It usually uses the antenna last used for successful transmission. In models with external antennas, sometimes only a single antenna is used. In this case, the **Transmit Antenna** should be configured to transmit only from that single antenna. Similarly, models using a booster or an LNA use only a single antenna for transmission. There are three possible options:
  - ❖ **Use Two Antennas**
  - ❖ **Use Antenna No. 1 only**
  - ❖ **Use Antenna No. 2. only**
- ◆ **Mobility:** BreezeNET PRO.11 stations optimize their roaming algorithms according to the mobility mode parameter. For example, a stationary station is more tolerant of bad propagation conditions. It assumes that this is a temporary situation and is not caused by the station changing position. Initiating a roaming procedure in such a case would be counter-productive.

In general, wireless stations can be used in one of three mobility modes:

- ❖ **High (Mobility):** Type **2** for stations that may move at speeds of over 30 km per hour.
- ❖ **Medium (Mobility):** Type **1** for stations that may move at speeds of over 10 km per hour, but not over 30 km per hour.
- ❖ **Low (Mobility):** Type **0** for stations that will not move at speeds of over 10 km per hour. **Stationary** is the default value, and in almost all cases this is the best choice.
- ♦ **Load Sharing:** Type **1** to enable Load Sharing. When installing a Wireless LAN network in a high-traffic environment, you can increase the aggregate throughput by installing multiple APs to create co-located cells. Load Sharing allows the wireless stations to distribute themselves evenly among the APs to best divide the load between the APs.

**NOTE:**

When working in Load Sharing mode, both the APs and the units should be configured to Load Sharing Enabled.

- ♦ **Preferred AP MAC (Ethernet) address of the preferred AP:** You can configure a station to prefer a specific AP unit. When the station powers up, it associates with the preferred AP even if the signal from that AP is lower than the signal from other APs. The station roams to another AP only if it stops receiving beacons from the preferred AP.
- ♦ **Use Prefix ESSID (for AP only):** This attribute defines whether the prefix ESSID feature is activated. The use of prefix ESSID enables association of stations with partial ESSID, adopting the full ESSID of the AP upon association.
- ♦ **Prefix ESSID (for AP only):** This attribute identifies the Wireless LAN prefix ESSID.
- ♦ **Station Mode (for SA only):** This attribute defines whether the station is activated as an Access Unit. A station activated as an Access Unit functions as a WB with only one PC behind it. The options are:

- ❖ **Access Station:** The Station functions as a WB with only one PC behind it
- ❖ **Use Host MAC Access Address for Association**
- ◆ **Display Current Values:** This read-only status screen displays the current WLAN parameters. Press any key to return to the *WLAN Parameters* menu.

## Bridging

The *Bridging* menu contains the following options:

- ◆ **LAN to WLAN Bridging Mode (AP Only):** The options are:
  - ❖ **Reject Unknown:** Type **0** to allow transmission of packets only to stations that the AP knows to exist in the Wireless LAN (behind the Wireless Bridge).
  - ❖ **Forward Unknown:** Type **1** to allow transmission of all packets except those sent to stations that the AP recognizes as being on its wired Ethernet side.
  - ❖ **Intelligent Bridging Period:** Intelligent bridging enables smooth roaming of WB-10 units. When intelligent bridging is enabled, the AP goes into a special bridging mode for a fixed amount of time whenever a wireless bridge (WB) roams into its area. This mode causes the AP to forward packets destined for the stations behind the WB-10 even though they are known or were learned from the wired side (except that no learning of the wired LAN will take place). Afterward, the AP switches back to **Reject Unknown** bridging mode. This procedure prevents packets destined for stations behind the bridge from getting lost. The value of this parameter is the length of time in seconds that the AP remains in the special mode.

**NOTE:**

When connecting very large networks, it is recommended to set this parameter to Forward Unknown.

- ◆ **IP Filtering:** Whether IP filtering is enabled for the unit. Enable **IP Filtering** to filter out any other protocol (such as IPX). Only IP traffic passes through the WLAN.
- ◆ **Tunneling:** Whether the unit performs tunneling. Enable Appletalk tunneling if the network contains a mix of Ethertalk1 (ET1) and Ethertalk2 (ET2) stations to ensure smooth communications. Enable IPX tunneling if IPX protocol is running over your network. Be sure to set all units to the same tunneling setting.
- ◆ **Broadcast Relaying (AP Only):** Whether the unit performs broadcast relaying. When **Broadcast Relaying** is enabled, Broadcast packets originating in WLAN devices are transmitted by the AP back to the WLAN devices, as well as to the LAN. If it is disabled, these packets are sent only to the local wired LAN and are not sent back to the WLAN. Disable **Broadcast Relaying** only if you know that all Broadcast messages from the WLAN will be destined to the wired LAN.
- ◆ **Unicast Relaying:** Whether the unit performs Unicast relaying. When **Unicast Relaying** is enabled, Unicast packets originating in WLAN devices can be transmitted back to the WLAN devices. If this parameter is disabled, these packets are not sent to the WLAN even if they are intended for devices on the WLAN. Disable **Unicast Relaying** only if you know that all Unicast messages from the WLAN will be destined to the local wired LAN.
- ◆ **Association Aging Period:** Units inactive for a period of time (in minutes) as defined in this parameter are disconnected.

## Station Control

The *Station Control* menu contains the following options:

- ◆ **Reset Unit:** Type **1** to reset the BreezeNET PRO.11 unit and apply any changes made to the system parameters.
- ◆ **Load Defaults:** When this option is implemented, system parameters revert back to the original factory default settings. There are two options:
  - ❖ **Load Full Factory Defaults:** All parameters revert to defaults except for Japan Call Sign (if applicable) and Hopping Standard.
  - ❖ **Load Partial:** All parameters revert to defaults, except for Japan Call Sign (if applicable), IP Address, Subnet Mask, Default Gateway, Hopping Sequence, Hopping Set, ESSID, Transmit Diversity, Long Range, Preferred AP, IP Filtering, Hopping Standard, Power Level, Auto Calibration, Encapsulation, WEP Attributes, Authentication Algorithm, Pre-authentication, WEP Default Keys, Ethernet Disable, Trap Host Addresses.

## Security (Authentication Feature)

Wired Equivalent Privacy (WEP) is an authentication algorithm that protects authorized Wireless LAN users against eavesdropping. The definition of WEP is defined in the 802.11 standard.

WEP, also referred to as the **Privacy** option, must be ordered specifically and is not supported by default. The security mechanism involves configuration of the following parameters:

- ◆ **Authentication Algorithm:** This module operates in two modes:  
**0-Open System** (default): no authentication; OR **1-Shared Key** authentication (for systems that have the privacy option implemented).

- ◆ **Default Key ID:** The key to be used for the encryption of transmitted messages.
- ◆ **Pre-authentication:** Set this parameter to **Enabled** when there is a great deal of roaming between the APs. Pre-authentication must be activated on both the APs and the stations.
- ◆ **Privacy Option Implemented: Yes** if **Shared Key** authentication is supported, No if Shared Key authentication is not supported.
- ◆ **WEP Key# 1-4:** The default encryption key must be set before you can use the Shared Key Authentication mode. The encryption key you enter for the AP, must match those defined in the stations. Each key is a combination of 10 Hex digits.

**NOTE:**

It is recommended to change the encryption keys periodically, to enhance system security.

## Advanced Settings Menu

The *Advanced Settings* menu enables you to configure parameters related to the system performance, translation mode, roaming capabilities, radio parameters, data rates, AP redundancy settings, maintenance configuration and voice and data parameters. Modification of most of the parameters in the *Advanced Settings* menu is limited to certified Alvarion engineers only.

```
BreezeNET PRO.11 Series (AP-10 D)
Version : 5.10
Tue Oct 17 12:58:47 2000

Advanced Settings menu
=====
1 - Translation Mode
2 - Roaming
3 - Performance
4 - Radio
5 - Rate
6 - AP Redundancy Support
7 - Maintenance
8 - Voice and Data Configuration
Select option >
```

**Figure 3-4: Advanced Settings Menu**

### Translation Mode

The translation mode determines how the unit handles 802.3 packets. The translation mode is either enabled (default) or disabled.



## Roaming

The *Roaming* menu is used to set various parameters regarding roaming and scanning in the wireless network. The roaming feature enables network connection to be maintained while roaming between overlapping coverage areas. Transmission and reception can be continued while moving at high speeds with no data packet loss or duplication. In order to verify that no packet loss occurs, the station scans all frequencies and checks the quality of neighboring APs before deciding whether it can switch to the coverage area of another AP.

- ◆ **Max. Number of Scanning:** The number of times a station scans to attempt to find a neighboring AP. If, after the maximum number of scans, no AP is found, the station performs a reset. A value of zero implies no reset.
- ◆ **Roaming Decision Window:** The minimum number of RSSI samples that is required to make a decision about the current WLAN channel quality (i.e., when to switch APs). A new RSSI sample arrives with each incoming frame.
- ◆ **Roaming Decision Numerator:** The maximum number of RSSI samples that are allowed to be below the **Roaming Decision RSSI Threshold**, among a number equal to Roaming Decision Window of the last arrived samples. If a number of bad samples (i.e. below Roaming Decision RSSI Threshold) exceeds this parameter setting, the channel is considered to be BAD.

**TIP:**

It is recommended not to adjust this value, as the factory default has been tested and has proven to be optimal for a majority of system configurations.

- ◆ **Roaming Decision RSSI Threshold:** An RSSI sample that is below this value is considered BAD, incrementing the Roaming Decision Numerator value by 1.

- ◆ **Joining Decision RSSI Threshold:** A station joins a new AP only if the AP transmits with an RSSI quality above this value. If a station associated with the AP is heard at an RSSI level below this threshold, a trap is sent by the AP.
- ◆ **Number of Beacons for Disconnect Decision:** Defines the maximum number of consecutive unsuccessfully received beacons before a disconnect decision is made.
- ◆ **Number of Probe Responses:** The number of acceptable scans (above the *Joining Decision RSSI Threshold*) required to move to the coverage area of a neighboring AP.

**TIP:**

In environments with a great deal of mobility (i.e., a great deal of roaming), it is recommended that you increase the value from the default.

- ◆ **Neighboring Beacon Rate:** Once in how many dwell times the AP sends a neighboring beacon. A value of zero implies no neighboring beacons.

**TIP:**

In environments with no mobility (i.e., no roaming), you can set this parameter to 0.

## Performance

The *Performance* menu determines the unit performance:

- ◆ **Dwell Time (AP Only):** The time spent on a radio channel before hopping to the next channel in the sequence.
- ◆ **RTS Threshold:** Minimum packet size to require an RTS. For packets with a size below the *RTS Threshold* value, an RTS is not sent and the packet is transmitted directly to the WLAN.
- ◆ **Max Multicast Rate:** Multicast and Broadcast transmissions are not acknowledged, therefore the chance of error increases. By default, the unit always transmits broadcasts, multicasts and control frames in the minimum possible rate, 1Mbps.

- ◆ **Power Save Support:** If you enable **Power Save Support** on one of the WLAN stations (SA-PCR only), you must also configure the AP unit. **Power Save Support** is influenced by two parameters:
  - ❖ **DTIM interval on the AP side:** Determines at which interval the AP sends its broadcast traffic (default 4 beacons).
  - ❖ **Listen interval on the SA-PCR side:** Determines when the station “wakes up” to listen to unicast packets that are destined to it (default value: 4 beacons).
- ◆ **DTIM Period:** Determines at which interval the AP sends its broadcast traffic to all the stations in the cell, both stations that are in power save mode and to stations that are not in power save mode (normal mode). When stations in power save mode “wake up” to receive broadcast frames, they can also poll the AP for the unicast frames if there are any stored in the AP’s buffer. Default value is 4 beacons (approximately every 1 second).
- ◆ **IP Stack:** By default this parameter is disabled, to check connectivity. Any changes to this parameter are returned to the default value whenever the unit resets.
- ◆ **Acknowledge Delay:** Enlarges the range of the system but can only be enabled for links above 20kms. It must be enabled on both sides. The values are **Long** or **Regular** (default) and can be configured by an Installer or Technician.
- ◆ **Beacon Interval:** A beacon is sent every number of dwells as defined in this parameter (default: 2 dwells).
- ◆ **Contention Window:** This parameter should be set according to the amount of hidden stations. Hidden stations are most prevalent in access applications (e.g. ISPs). The greater the number of hidden stations, the larger the initial size of the contention window should be set. Possible values are **7, 15, 31, 63**. The default value is 7.

- ◆ **Associate with AP Running S/W Version 4.X and below:** This parameter is only relevant for WB units. Enabling this parameter causes the broadcast, sent by the WB, to be preceded by a relatively large back off period, since APs from Versions 4.x and up can not receive frames in high rate (in bursts).

## Radio

The *Radio* menu contains the following parameters:

- ◆ **Hopping Standard:** The *Hopping Standard* is a set of rules regarding the radio transmission standard allowed in each country. Units work together only if set to the same hopping standard. Use this parameter to set the unit's hopping standard to that of the relevant country.
- ◆ **Display Site Propriety Sequences:** The site proprietary frequencies are displayed for each hopping set.
- ◆ **Power level:** Output power level at which the unit is transmitting. There are two possibilities, **Low** (10dBm) or **High** (17 dBm) at the antenna connector.
- ◆ **Carrier Sense Level:** This attribute defines the carrier sense absolute threshold. When sample are above this level, the media is considered to be busy.
- ◆ **Carrier Sense Differential Level:** This attribute defines the carrier sense differential threshold, which defines at which level the received signal is considered to be a packet.
- ◆ **Noise Floor:** Defines the level above which a received signal is considered to be a packet.
- ◆ **External Amplifier:** Whether or not an external amplifier is used.

## Rate

The *Rate* menu comprises the following parameters:

- ◆ **Multi-Rate Support:** When this parameter is enabled, the unit automatically switches to the best transmission rate at any given time. When the parameter is disabled, the unit always stays at the maximum rate configured in the *WLAN Parameters* menu.
- ◆ **Multi-Rate Decision Window Size:** The number of successful transmissions required before the unit automatically switches to the next highest transmission rate.

## AP Redundancy Support

When the AP identifies that the Ethernet link has been or there is no traffic on the Ethernet side over a defined period of time, it then stops transmitting and forces the stations associated with it to associate with another AP.

The default mode for the **AP Redundancy Support** parameter is disabled (the AP continues transmitting even when the ETH link is discontinued). This can only be configured by a Technician. It is recommended to use this parameter only when more than one AP is connected to the same distribution system and this AP is configured to the same ESSID.

## Maintenance

The Installer has access to modify the following parameters in the *Maintenance* menu:

- ◆ **Wait for Association Address:** This attribute indicates which MAC address the station uses when associating the AP. Two values are possible:

- ❖ **Use mine:** The station tries associating the AP with its own MAC address; this option enables managing the unit but does not enable communication with the PC behind the Station.
- ❖ **Wait for update via Ethernet:** The unit tries associating the AP with the MAC address of the PC behind it; this occurs only after the PC behind the station has tried communicating.
- ◆ **Japan Call Sign:** The *Japan Call Sign* is part of the Japanese standard, defined according to local regulations. The Japanese Ministry of Communications supplies an activation code for the units; this code is set in the factory for each unit.

## Voice and Data Configuration

The *Voice and Data Configuration* menu is comprised of the following parameters:

- ◆ **Enable Voice:** When enabled, voice packets are given priority over data packets. If packets are discarded, data packets are discarded first.
- ◆ **Max Number of Retransmissions in Voice Packets:** The number of times the voice frame is retransmitted, during the last dwell, before it is dropped. For example, if the *Number of Dwells to Retransmit* parameter (see next) is **2** and the *Max Number of Retransmissions* is set to **10**, the station retransmits 10 times during the third dwell. If unsuccessful, the frame is dropped.
- ◆ **Number of Dwells to Retransmit in Voice Packets:** The number of dwells during which the station attempts to retransmit voice packets.
- ◆ **Max Number of Retransmissions in Data Packets:** The number of times the data frame is retransmitted, during the last dwell, before it is dropped.
- ◆ **Number of Dwells to Retransmit in Data Packets:** The number of dwells during which the station attempts to retransmit data packets.

## Site Survey Menu

The *Site Survey* menu enables you to gather performance statistics for the selected unit. This helps in positioning your units and aligning the antennas of the units, as well as troubleshooting.

```
BreezeNET PRO.11 Series (SA-10 DL)
Version : 5.10
Tue Oct 17 12:58:47 2000
Site Survey menu
=====
1 - System Counters
2 - Survey Software
3 - Event Log
4 - Display Neighboring AP's
Select option >
```

**Figure 3-5: Site Survey Menu**

## System Counters

The System counters are a simple yet efficient tool for monitoring, interpreting and analyzing the Wireless LAN performance. The counters contain statistics concerning Wireless and Ethernet frames. The sub-menu contains the following options:

- ◆ **Display Ethernet and WLAN Counters:** Choose this option to display the current value of the Ethernet and Wireless counters. Refer to Ethernet Counters, on page 3-32, and *Wireless LAN Counters*, on page 3-33, for a detailed description of the counters.

- ◆ **Display Rate Counters:** Displays contents of packets at each rate. The AP displays counters per station.
- ◆ **Display Rx Packets per Frequency:** Two display options are available: table format and histogram format. Refer to *Using the Rx Packets per Frequency Histogram*, on page 3-36 for more information.
- ◆ **Reset Counters:** Choose this option to reset all counters. After choosing this option you are requested to type **1** for confirmation or **0** to cancel the reset.
- ◆ **Power Saving Counters:** Displays the power saving counters per station, the number of transmitted frames and the number of discarded frames. This applies only to APs.
- ◆ **Display Quality Counters:** For APs, displays information of all associated units. The information is displayed as a table and includes the following: the MAC address of the associated unit, the RSSI and dBm of the unit as heard by the AP (collected from Acknowledge frames received by the AP from the unit).  
For other units: the information is displayed as a table and includes: the MAC address of the AP the unit is associated to, the RSSI and dBm of the AP as heard by the unit (collected from Acknowledge frames received by the unit).

## Ethernet Counters

*Ethernet Counters* display statistics about the unit's Ethernet port activity.

The unit receives Ethernet frames from its UTP port and forwards them to its internal bridge, which decides whether or not to transmit them to the Wireless LAN. The units have a smart hardware filter mechanism which filters most of the frames on the LAN, and hardware filtered frames are not counted.



On the other side, frames received from the wireless LAN and some frames generated by the unit (answers to SNMP queries and pings which reached to the unit via the UTP port), are transmitted to the UTP port.

#### Available Counters

- ♦ **Frames Received:** Total number of frames received from the Ethernet port.
- ♦ **Bad Frames Received (sum and percent):** The number and percentage of frames received from the UTP port. A large number of received bad frames indicates a problem in the UTP connection such as a bad UTP cable or hub port.
- ♦ **Missed Frames (internal overflow):** Frames that were recognized by the unit, but failed to be read since no available free buffer was located.
- ♦ **Transmitted to Ethernet:** The number of frames transmitted by the unit to the UTP port. i.e., frames that have been received from the Wireless side, and frames generated by the unit itself.

## Wireless LAN Counters

*Wireless Counters* display statistics about the unit's Wireless LAN activity.

Transmission to the wireless media includes data frames received from the UTP ports, as well as self generated control and management frames. When a data frame is transmitted, the unit will wait for an acknowledge from the receiving side. If an acknowledge is not received, the unit will retransmit the frame until it gets an acknowledge (there are no retransmissions for control frames). If the unit has retransmitted a frame for the maximum number of retransmissions it will stop re-transmitting the frame and drop this frame.

### Available Counters

- ◆ **Total Frames Transmitted Successfully:** The total number of frames transmitted successfully, not including retransmissions.



#### NOTE:

An AP continuously transmits a control frame called beacon in every frequency to which it hops, in order to publish its existence and keep its associated stations synchronized. Thus, the total transmitted frames counter will get high values even if the AP-10 is not connected to an active LAN.

- ◆ **Total Frames Retransmitted (sum and percent):** X = total number of frames retransmitted. P = percentage of frames retransmitted from the total number of transmitted frames.
- ◆ **Data Frames Transmitted (including Retransmissions):** The number of data frames transmitted successfully, not including retransmissions.
- ◆ **Data Frames Retransmitted (sum and percent):** X = number of data frames retransmitted. P = percentage of data frames retransmitted from the total number of transmitted frames.
- ◆ **Total Frames Transmitted (including retransmitted):** Total number of frames transmitted including retransmitted frames.
- ◆ **Frames Dropped (too many retries):** The number of dropped frames. Frames are dropped when they were retransmitted for the maximum allowed retransmission attempts.
- ◆ **Frames Discarded (Internal overflow):** The number of frames discarded from the WLAN port, due to buffer overflow. Frame discard will occur when the wireless conditions are bad, the unit is busy re-transmitting frames, and is not able to handle new frames.
- ◆ **Power Saving Aged:** Total number of buffered frames that were aged out. This counter counts the number of frames dropped by the AP because a station did not poll those frames for a long period of time.
- ◆ **Frames Received (data + management):** The number of frames received from the wireless media. The count includes data and control frames (including beacons received from APs).

- ◆ **Data Frames Received:** The number of data frames received from the wireless media.
- ◆ **Bad Frames Received (sum and percent):** The number and percentage of frames received with CRC error
- ◆ **Duplicated frames received:** When a unit receives a frame it sends an acknowledge for it. If the acknowledge is lost, it receives a copy of the same frame. Although duplicate frames are counted, only the first copy of the frame is forwarded to the UTP port.
- ◆ **Total Frames Received:** Total number of received frames.
- ◆ **Probe Response sent (AP only):** The total number of Probe Response frames sent by the AP to requesting units.
- ◆ **Probe Response received (SA only):** The number of Probe Response received by the unit (sent by responding APs).
- ◆ **Probe Request sent (SA only):** The number of Probe Request frames sent by unit.
- ◆ **Probe Request Received (AP only):** The number of Probe Request received by the AP (from requesting units).
- ◆ **Auth Request sent (SA only):** The number of Authentication Requests sent by the unit.
- ◆ **Auth Request Received (AP only):** The number of Authentication Requests received by the AP (from requesting units).
- ◆ **Assoc Response sent (AP only):** The number of Association Response frames sent by the AP to requesting units.
- ◆ **Assoc Response received (SA only):** The number of Association Response frames received by the unit (sent from the AP).
- ◆ **Assoc Request Sent (SA only):** The number of Association Request frames sent by the unit to AP.
- ◆ **Assoc Request Received (AP only):** The number of Association Request frames received by AP from requesting units.

## Display Rate Counters

The *Rate Counters* display the number of frames transmitted in each data-rate since the last reset. As displayed, the rate counters show the number of frames transmitted at 1Mbps, 2Mbps, 3Mbps, and the number of Re-Transmitted frames (Ret). The counters display the rate of packets transmitted for the first time only (without retransmissions).



### NOTE:

Counters for APs are displayed for all associated stations, indicated by their MAC address. Rate counters for stations are displayed with no indication of MAC address.

00-20-D6-12-88-4E: Data tx on rates 1Mb: 23; 2Mb: 67; 3Mb: 462; Ret: 30
00-20-D6-12-25-13: Data tx on rates 1Mb: 250; 2Mb: 550; 3Mb: 0; Ret: 29

**Figure 3-6: Rate Counters**

Checking the Rate Counters is the best way to determine which data-rate is the optimal data-rate for the unit. It is recommended to restrict the Maximum Data Rate for each unit according to the Rate Counters. The Rate Counter displays the number of frames that had to be retransmitted, however it does not count the number of retransmissions that actually accrued.

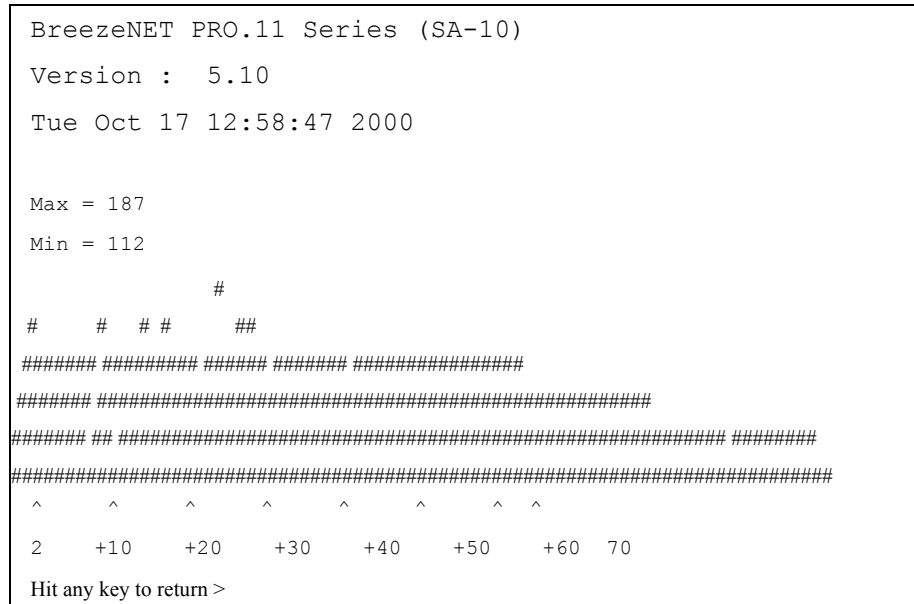
## Using the Rx Packets per Frequency Histogram

Use one of the ***Display Rx Packets per Frequency*** options to see a histogram of the number of frames received on each channel. This menu provides the following options:

- ◆ **Display Rx packets per frequency Table:** Displays the number of frames received at each frequency in table form; the table includes an index, the frequency and the number of frames received in this frequency.

- ◆ **Display Rx packets per frequency Graph:** Displays a histogram of the number of frames received on each channel. This option is not available for the site proprietary hop standard.

The following is an example of the histogram.



**Figure 3-7: Display Rx Packets per Frequency**

Each point of the histogram line corresponds to a frequency. The base frequency appears at the far left, and gradations are marked in steps of ten along the line. A hash (#) represents each packet received on a given frequency. The Max and Min values indicate the highest and lowest number of frames received across all frequencies. This graph is very useful for tracking interference. Frequencies with small numbers of packets received probably have more interference than other frequencies.

## Reset All Counters

This option enables you to reset the system counters, Ethernet counters, WLAN counters, and Rate counters.

- ◆ Click **1** to reset all counters.
- ◆ Click **0** to cancel request.

## Power Saving Counters

These counters apply only to APs.

- ◆ **PS stations:** Number of associated stations currently working in Power Save mode.
- ◆ **Internally Discarded:** Number of frames that were discarded because of aging.
- ◆ **Table:** Valid only when Power Save mode is enabled.
  - ❖ **Station ID:** The station ID in the power save table.
  - ❖ **Buffered:** Number of buffered frames per station.
  - ❖ **Aged:** Number of buffered frames that were aged out from buffer, per station.
  - ❖ **Sent:** Number of buffered frames that were sent to a specific station.
  - ❖ **Queue Full:** Number of frames that could not be stored in the buffer.

## Survey Software

The *Survey Software* menu enables you to align antennas and to assess the radio signal quality of a point-to-point link. The sub-menu includes the following options:

- ♦ **Operation Mode:** When running a Site Survey, set the units on either side of the link to either receive (option 1) or transmit (option 2) packets (one unit should be set to transmit and the other to receive).
- ♦ **Start Statistics:** Type **2** and then press any digit to start Site Survey.
- ♦ **Stop Statistics:** Type **3** and then press any key to stop update of Site Survey statistics.

## Using the Site Survey Software

The following procedure describes how to perform a site survey using the BreezeNET 5.00 new Site Survey software.

- 1.** Roughly align the antennas on either side of the link before starting the Site Survey procedure.
- 2.** Verify that the Ethernet cables are disconnected from both units.
- 3.** Type **1** to access the *Operation Mode* screen. Set the units on either side of the link to either receive (option 1) or transmit (option 2) packets (one unit should be set to transmit and the other to receive).
- 4.** Start the survey by typing **2** in the *Survey Software* menu in both units. When performing a site survey from a station to an AP (transmitting from the station to the AP), always begin with the station (type 2 on the station).

5. On the transmit side, a table appears displaying the number of packets and the frequency at which each packet was transmitted.

This list is updated continuously.

BreezeNET PRO.11 Series (SA-10 DL)		
Version : 5.10		
Tue Oct 17 12:58:47 2000		
#	Tx	Packets Channel
0	37	
1	10	
2	7	
3	30	
4	28	
5	44	
6	35	
7	12	
8	48	
9	76	
10	42	
Hit any key to return >		

**Figure 3-8: Transmit Statistics**

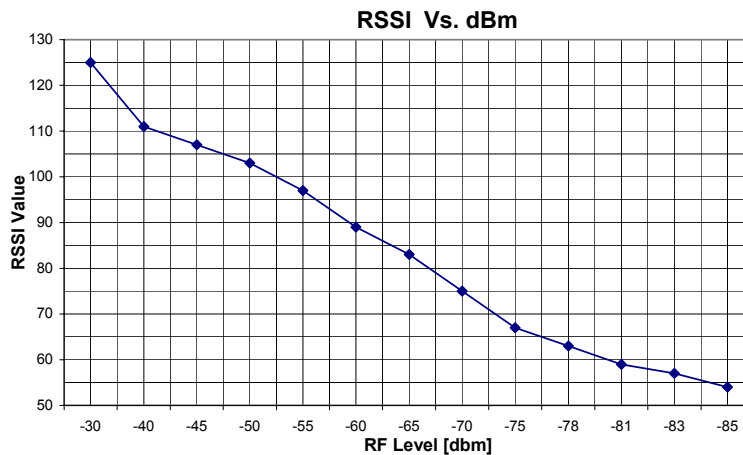


6. On the receive side of the link, the screen displays a table showing the packet number received, the frequency at which each packet was transmitted, the Received Signal Strength Indicator (RSSI) for each antenna and the antenna that was selected for reception (refer to Figure 3-8). Use only the RSSI reading from the selected antenna.

#Pack	Ant	RSSI1	RSSI2	Bit_Err	Freq	Rate	Quality
105	1	92	84	0	76	2	#####..
106	1	92	82	0	75	2	#####..
107	1	89	89	0	58	2	#####...
108	1	95	92	0	51	2	#####.
109	1	95	89	0	46	2	#####.
110	1	95	81	0	10	2	#####.
111	1	95	90	0	31	2	#####.
112	1	95	51	0	4	2	#####.
113	1	92	85	0	5	2	#####.
114	1	99	90	0	77	2	#####.
115	1	102	89	0	43	2	#####.
116	1	95	89	0	22	2	#####.
117	1	105	86	0	58	2	#####.
118	1	103	89	0	51	2	#####.
119	1	102	89	0	46	2	#####.
120	1	104	69	0	64	2	#####.
121	1	97	87	0	78	2	#####.
122	1	100	87	0	33	2	#####.
123	2	87	85	0	71	2	#####...
124	2	82	85	0	70	2	#####...

**Figure 3-9: Receive Statistics**

7. The RSSI is given in arbitrary units. Use the graph in Figure 3-9 to correlate RSSI to dBm.



**Figure 3-10: RSSI to dBm Graph**

8. Re-align the antennas until the maximum received signal strength is attained. As you align the antennas, the RSSI (received signal strength indicator) continually increases until it reaches a certain level after which the RSSI begins to decrease. This is the maximum attainable RSSI level indicating optimum receive antenna alignment.
9. Switch the functions of either side of the link (set the transmit unit to receive and the receive unit to transmit) and repeat the procedure to check the link from the opposite direction.
10. To stop the survey/statistics, press any key and then select the **3-Stop Statistics** option from the *Survey Software* menu.

## Event Log

The *Event Log* records all the error messages that the unit displayed since the last Load Full Factory Defaults reset or since the log was erased by Erase Event Log. The Event log stores events in four levels of error notifications: MSG (Message), WRN (Warning), ERR (Error), and FTL (Fatal).

The following options are available in this screen:

- ◆ **Show All Messages:** Displays all messages.
- ◆ **Show Information severity and higher:** Display all messages from informational level up.
- ◆ **Show Warning severity and higher:** Display all messages from warning level and up.
- ◆ **Show Error severity and higher:** Display all messages from error level and up.
- ◆ **Show Fatal Errors Only:** Display all messages from fatal error level and up.
- ◆ **Complete Mask-Don't Display Any Type of Message:** No messages are displayed.

➤ **To display the event log:**

- 1.** From the *Main* menu select **3** to open the *Site Survey* menu.
- 2.** Select **3** to display the *Event Log* sub-menu.
- 3.** Select **1** to display the Display Event Log selection screen.
- 4.** Enter the number of events to display, and press any key.

The Event Log starts to list the most recent events according to the number of you have entered. For example if you entered 100, the event log displays the last 100 events.

## Display Neighboring APs

Displays neighboring APs on the same ESS for both the AP and station units.

## Access Control Menu

*Access Control* functions enable the System Administrator or Installer to limit access to Local Terminal Maintenance setup and configuration menus.

```
BreezeNET PRO.11 Series (SA-10)
Version : 5.10
Tue Oct 17 12:58:47 2000
Access Control menu
=====
1 - Change Access Rights
2 - Change Installer Password
3 - Change Write Community Password
4 - Change Read Community Password
S - Show Current Access Right
Select option > 1
```

**Figure 3-11: Access Control Menu**

The *Access Control* menu includes the following options:

- ♦ **Change Access Rights:** This screen determines the level of access rights to the BreezeNET PRO.11 unit's setup and configuration menus. When the unit is first installed, the default access right is **Installer**, and the default password is **inst2000** (case sensitive).

- ❖ **User:** The *Local Terminal Management* menus are read-only for a user who does not possess the correct password. The ESSID and security parameters are hidden by asterisks (\*) at this level.
- ❖ **Installer:** The installer has access to configure all required parameters in the system configuration menu, as well as some of the advanced settings. Access is password-protected. After configuration, the installer should change access rights to option (0), User. The installer can also change the installer password (see next parameter).
- ❖ **Technician:** Only a Certified Alvarion Engineer possessing the correct password can select this option to configure all the parameters and settings.
- ◆ **Change Installer Password:** Type in the new password according to the directions on screen. This screen changes the installer password to prevent unauthorized persons from making any changes in system configuration and setup. The password is limited to eight printable ASCII characters. This option is not available at User level.
- ◆ **Change Write Community Password:** Enables you to change the SNMP Write Community Password of the unit. The default password is **Private**.
- ◆ **Change Read Community Password:** Enables you to change the SNMP Read Community Password of the unit. The default password is **Public**. To change the passwords, you will need the Installer access rights (and up).
- ◆ **Display Current Access Right:** This read-only screen presents the current access right configuration.

## Code Activate Control Menu

The embedded software of the PRO.11 unit is stored on a Flash memory component. The Flash components houses two memory banks: an active bank (the version that is currently running) and a non-active backup bank. The *Code Activate Control* menu allows you to perform the following options:

- ♦ **Try To Run From Non-Active Code:** The unit tries to run from the non-active code. An appropriate message is displayed if the switch is successful; or an error message is displayed if not.
- ♦ **Check Non-Active Code State:** Checks the non-active, backup, memory bank CRC and returns the code state (Good or Bad).









# Chapter 4

## SA-PCR PRO.11

### PC Card

### Installation,

### Setup, and

### Management

#### About This Chapter

This chapter describes how to install the SA-PCR card and its associated firmware, drivers and utilities. The SA-PCR Configuration and SA-PCR Site Survey utilities, which are used to setup and manage the card, are also described in this chapter.

This chapter is comprised of the following sections:

- ♦ **Packing List**, page 4-3, lists the items included in the installation kit.
- ♦ **Before You Begin**, page 4-3, provides a list of the considerations that must be taken into account before installation.
- ♦ **Installing the SA-PCR Card**, page 4-4, describes how to install the physical card component.
- ♦ **Installing the SA-PCR Utilities**, page 4-22, describes how to install the card software components.

- ◆ **Using the SA-PCR Configuration Utility**, page 4-28, describes how to use the configuration and management application.
- ◆ **Using the Windows CE SA-PCR Utility**, page 4-45, describes how to use the Windows-based application.
- ◆ **Using the SA-PCR Site Survey Utility**, page 4-48, describes how to use the monitoring and statistics application.
- ◆ **Using the Upgrade Kit Program**, page 4-54, describes how to upgrade the card software.
- ◆ **Installation Troubleshooting**, page 4-61, provides answers to the most common issues that may be encountered during installation.
- ◆ **Installing the SA-PCR Drivers in ODI Systems**, page 4-62, describes how to operate the card software on ODI systems.
- ◆ **Installing the SA-PCR in Linux Systems**, page 4-66, describes how to install and operate the card software on Linux systems.

## Packing List

The SA-PCR PRO.11 installation kit includes the following items:

- ◆ SA-PCR PRO.11 PC card
- ◆ Drivers diskette
- ◆ Utilities diskette
- ◆ Installation and User's Guide

## Before You Begin

Before installing, consider and execute the following:

- ◆ Verify that the AP you are using is an AP-10 PRO.11. The SA-PCR PRO.11 operates with any AP that is compliant to the 802.11 standard.

It is advisable to turn on the AP before installing the SA-PCR, enabling you to use the SA-PCR LEDs to check the status of the SA-PCR when installation is complete.

- ◆ **When installing on Windows 95/98**, verify that you have the Windows CD with you, or that the Windows CAB files are installed on your local hard disk in a directory whose name does not exceed 8 letters. When the CAB files are on the disk, they are usually found in C:\Windows\Options\Cabs.
- ◆ **When installing on Windows NT**, verify that you have the Windows NT CD with you, or that the Windows NT distribution files are installed on your local hard disk. During installation, enter the path of the distribution files whenever a message appears requesting this information.

- ◆ It is highly recommended that you **remove all PCMCIA cards from the notebook prior to installing the SA-PCR card**. This will help to avoid conflicts during installation. If you have another network card installed (e.g., an Ethernet card), you must remove it prior to installing the SA-PCR card.

## Installing the SA-PCR Card

Installing the SA-PCR PRO.11 card consists of the following steps:

- ◆ Installing the card in a PCMCIA slot
- ◆ Installing the SA-PCR drivers and utilities

*Initial Configuration*, on page 4-21 provides instructions on performing initial configuration of the SA-PCR card. *Using the SA-PCR Configuration Utility*, on page 4-28, provides installation troubleshooting information.



### NOTES:

If you are installing the card with Windows 95 or Windows 98 systems, there are two installation options. You can install the drivers and utilities separately, or you can use the Upgrade kit program to install all components in one session. The upgrade kit program is described in *Using the Upgrade Kit Program*, on page 4-54.

**If you are installing the card with Windows CE**, you will need to connect the handheld PC to its host desktop PC in order to install the drivers. This procedure is described on page 4-17.

## Installing the SA-PCR Drivers

The SA-PCR card can be installed to operate with a wide range of PC operating systems. The following table lists the supported operating systems, together with the page number in the user's guide which describes the relevant installation procedure. Skip to the page that describes the relevant procedure.

If you are installing the SA-PCR with:	Refer to:
Windows 2000	page 4-6
Windows 98	page 4-10
Windows 95A	page 4-13
Windows 95B	page 4-13
Windows NT	page 4-15
Windows CE	page 4-17
ODI (DOS)	page 4-62
Linux	page 4-66

## **Installing the SA-PCR Driver for Windows 2000 Systems**

This section describes the software installation of the SA-PCR station adapter in PCs running the Windows 2000 operating system.


To perform this procedure, you will need the driver kit, which consists of the BRZW2KA.EXE file. Running this file installs both the SA-PCR driver and the BreezeNET Configuration Utility (a Windows Control Panel applet). You can download the driver kit from [www.alvarion.com](http://www.alvarion.com). Call Alvarion customer support for further information.

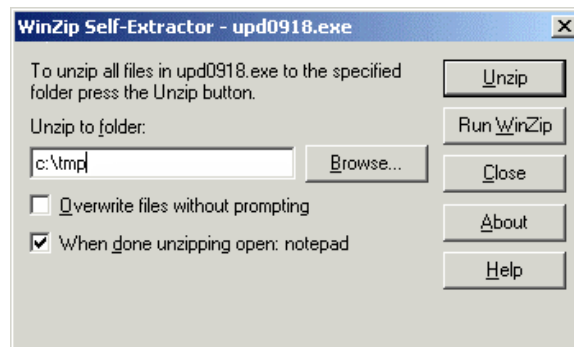
When installing certain models of the card with Windows 2000, the system automatically installs the SA-PCR driver on the Microsoft Windows 2000 Installation CD. This driver has restricted capabilities and is not compatible with some BreezeNET features (such as the Configuration Utility). To install a driver that is fully compatible with all BreezeNET features, perform the upgrade procedure described in the following section.

## Installing the Windows 2000 Driver Kit

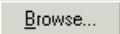
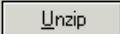

Installing the SA-PCR driver for Windows 2000 requires the Windows 2000 Driver kit

### ➤ To install the Windows 2000 Driver Kit:

1. Run the BRZW2KA.EXE file. Click  when prompted. The following window is displayed.



**Figure 4-1: Installing the Windows 2000 Driver Kit**

2. By default, the driver kit program extracts the files to the TMP directory of your default hard drive. To change the location, enter the path in the *Unzip to folder* field or click  and navigate to the required directory.
3. Click  to start extracting, or click  to open the Winzip application if you need to control the extraction process. After extraction, a message is displayed informing you that the files were extracted.

## Installing SA-PCR Cards With Windows 2000

This section describes how to install the SA-PCR Cards for PCs running Windows 2000.

### ➤ To install the SA-PCR Cards With Windows 2000:

1. Physically install the SA-PCR card.
2. Start the PC and login to the system with Administrator access rights. A *Found New Hardware* message is displayed.
3. Follow the instructions provided by the *Add Hardware Wizard* and when prompted, navigate to the driver file installed by BRZW2KA.EXE (located in C:\TMP by default).



#### NOTE:

If Windows 2000 does not ask you to specify the location of the driver and installs one automatically from the Windows 2000 CD, perform the procedure described in the following section.

4. If Windows displays the *Digital Signature Not Found* message, click **Yes**. This update may contain drivers that are not digitally signed.
5. After the driver installation is complete, open the Configuration Utility and select the required ESSID and country code.
6. If you do not need to restart Windows, eject the card and insert it again. The device will now work with the updated driver. The new settings become effective after the card is removed and inserted again, or Windows is restarted.




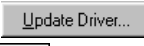



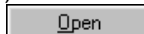


#### IMPORTANT:

Before removing the card, be sure to perform the Stop function from the Removable devices Taskbar icon. This icon is normally visible if removable devices are attached to your PC. Removal of a device without stopping it first can crash Windows and cause the loss of your data.



## **Upgrading the Windows 2000 Driver for PnP SA-PCR Cards**

If Windows 2000 automatically installed the SA-PCR driver on the Microsoft Windows 2000 Installation CD, you must to perform the following upgrade procedure. The driver provided on the Windows 2000 Installation CD has restricted capabilities and is not compatible with some of the BreezeNET features (such as the Configuration Utility).

1. Open the Device Manager with Administrator access rights (if you have not logged in as an Administrator).
2. Expand the Network Adapters branch and select the BreezeNET Wireless LAN PC Card.
3. Click  and select the *Driver* tab of the *Properties* window.
4. Click . The *Update Device Driver Wizard* starts. Click .
5. Select the **Display a list of all drivers...** option and click .
6. Click .
7. Enter the location path and name of the driver or browse to the location where the driver can be found (C:\TMP by default). A list appears that contains exactly one item. Select it and click . Then click .
8. In the *Wizard is ready to install...* window click .
9. If Windows displays the *Digital Signature Not Found* message, click **Yes**. This update may contain drivers that are not digitally signed.
10. Click **Finish**.
11. After the driver update is complete, open the Configuration Utility from the *Control Panel*, by selecting **Settings** and then **Control Panel** from the Windows *Start* menu. Then, double click the **BreezeCOM Configuration** icon.

**12.** Select the required ESSID and country code.



**NOTE:**

If Windows prompts to restart, click YES and restart Windows; while Windows is shut down, remove the card (so you can use the Configuration Utility before the card starts).

**13.** If you do not need to restart Windows, eject the card and insert it again. The new settings become effective after the card is removed and inserted again, or Windows is restarted.



**IMPORTANT:**

If Windows prompts to restart, click YES and restart Windows; while Windows is shut down, remove the card (so you can use the Configuration Utility before the card starts). Before removing the card, be sure to perform the Stop function from the Removable devices Taskbar icon. This icon is normally visible if removable devices are attached to your PC. Removal of a device without stopping it first can crash Windows and cause loss of your data.

## ***Installing/Updating the Site Survey***

The Site Survey utility can be installed and updated as a separate package. Users do not need Administrator rights in order to install and run the application.



**IMPORTANT:**

Do not use the Win9x Site Survey utility with Windows 2000; only use the Windows 2000 Site Survey utility.

To install the Site Survey application, run the SURVEY.EXE file installed by BRZW2KA.EXE (located in C:\TMP by default).

## **Installing the SA-PCR Drivers in Windows 98**

This section describes how to install the SA-PCR drivers for PCs running Windows 98.

- 1.** Insert the SA-PCR card in a free PCMCIA slot. Windows detects the unit and displays the *New Hardware Found* window.
- 2.** When the *Add New Hardware Wizard* window appears, click **Next**.
- 3.** Select the **Search for best driver** option and click **Next**.

4. Insert the BreezeCOM drivers diskette, select the **Floppy disk drives** option and click **Next**.
5. The installation wizard notifies you that the driver for the BreezeNET Wireless LAN PC card has been located. Click **Next**.
6. A window appears notifying you that the driver for the BreezeNET Wireless LAN PC card has been installed. Click **Finish**.
7. Restart the computer.

➤ **To uninstall the SA-PCR Drivers in Windows 98:**

1. From the Windows *Start* menu, select **Settings**, and then select **Control Panel**. Double click the **Network** icon, click the **Configuration** tab, select **BreezeNET Wireless LAN PC card**, and click **Remove**. A message appears asking whether you want to restart the computer; click **No**.
2. Insert the BreezeCOM Drivers diskette. From the Windows *Start* menu, select **Run**, and type a:\DrvClean.
3. When notified that the SA-PCR driver has been deleted, click **Setup**.
4. Restart the computer.

## Installing the SA-PCR Drivers in Windows 95

This section describes how to install the SA-PCR drivers on a PC running Windows 95.

1. From the Windows 95 desktop, right-click the **My Computer** icon and select **Properties**. The *System Properties* window is displayed.



**Figure 4-2: System Properties Window – Windows 95B**

2. Click the *General* tab. The letter indicating the type of operating system (a or b) is displayed under the System heading.
3. If you are running the Windows 95A operating system, refer to the following *For Windows 95A* section. If you are running Windows 95B operating system, refer to the *For Windows 95B* section on page 4-13.

## Windows 95A

1. Insert the SA-PCR card in the PCMCIA slot on your computer. Windows 95 detects the unit and displays the *New Hardware Found* window.



**Figure 4-3: New Hardware Found Window**

2. Select the driver from disk provided by hardware manufacturer option and click **OK**.
3. When prompted for the location of the driver, insert the BreezeCOM drivers diskette, type A:\ and click **OK**. The necessary files are copied from the diskette.
4. When the *Please insert disk labeled Windows 95 CD-ROM* message appears, insert the Windows 95 CD and click **OK**. If the Windows 95 CAB files are located on your local hard disk, you can navigate to that directory (usually found in \Windows\Options\Cabs).
5. If this is the first time a network card has been installed on this PC, a network setup window may appear. It is not necessary to fill out this window for the purposes of this installation.
6. Restart the computer.

## Windows 95B

1. Insert the SA-PCR slot in the PCMCIA slot on your computer. Windows 95 detects the unit, briefly displays the *New Hardware Found* window, and then displays the *Update Device Driver Wizard* window.
2. Insert the BreezeCOM drivers diskette and click **Next**. When Windows 95 notifies it has found the driver, click **Finish**.
3. If the Windows 95 CAB files are not found automatically, the message *Please insert disk labeled Windows 95 CD-ROM* appears. Click **OK**.
4. If the file BRZCOM.VXD is not found, direct the window to drive A:\ and click **OK**.
5. If no other windows appear, the installation is complete. If the *Please insert disk labeled Windows 95 CD-ROM* message appears, click **OK**, enter the path of the Windows 95 CAB files, and click **OK**. Installation is now complete.
6. Restart the computer.

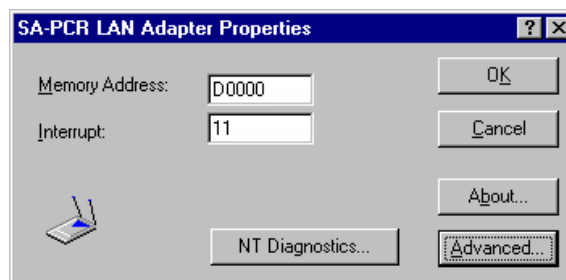
### ➤ To uninstall the SA-PCR drivers in Windows 95:

1. From the Windows *Start* menu, select **Settings - Control Panel**. Double click the **PC Card** icon, select **BreezeCOM Wireless LAN PC Card** and click **Stop**. Close all active applications. A message appears asking whether you want to restart the computer; click **No**.
2. From the Windows *Start* menu, select **Settings**, and then select **Control Panel**. Double click the **Network** icon, click the *Configuration* tab, select **BreezeNET Wireless LAN PC card**, and click **Remove**.
3. Insert the BreezeCOM Drivers diskette. From the Windows *Start* menu, select **Run**, and type a:\DrvClean.
4. When notified that the SA-PCR driver has been deleted, click **Setup**.
5. Restart the computer.

## Installing the SA-PCR Drivers in Windows NT

This section describes how to install the SA-PCR drivers in PCs running Windows NT.

1. Press the Windows **Start** button, select **Settings**, and then select **Control Panel**. Double-click on the **Network** icon.
2. If the message *The Windows NT Networking is not installed. Do you want to install it now?*, is displayed, continue with step 2a. If this message does not appear, continue with step 2b.
  1. Click **Yes** and choose **Wired to the network**. When a list of supported network adapters appears, click **Have Disk**.
  2. Click the *Adapters* tab, click **Add**, and then click **Have Disk**.
3. Insert the BreezeCOM drivers diskette, enter the location of the diskette (e.g., A:\) and click **OK**.
4. From the list select **BreezeNET Wireless LAN PC card** and click **OK**. The *SA-PCR LAN Adapter Properties* window is displayed.



**Figure 4-4: SA-PCR LAN Adapter Properties Window**

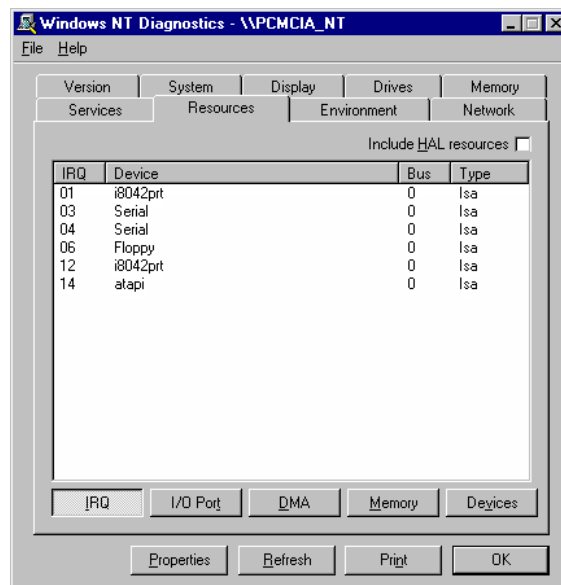
5. The default settings are memory range **D0000h** to **D3FFFh**, **IRQ 11**. In the following steps we will ensure that these default settings are acceptable for your machine.



**NOTE:**

If the SA-PCR Configuration utility is already installed, you can access it directly by pressing **Advanced**.

6. From the Windows *Start* menu select **Run**. Type WINMSD and click **OK**. The *Windows NT Diagnostics* window is displayed.



**Figure 4-5: Windows NT Diagnostics Window**

7. Click **IRQ** and verify that IRQ 11 is not taken. If it is, find a free IRQ. For example, in Figure 4-5 IRQ 5 is free.
8. Click **Memory** and verify that memory from D0000h to D3FFFh is not taken. If it is, find another free memory location, such as E0000h.
9. Return to the *SA-PCR LAN Adapter Properties* window. If the default values for **Memory Address** and **Interrupt** are acceptable, click **OK**. Otherwise, enter new values and click **OK**.
10. Click **Close** to close each installation window.
11. If configuration windows for other network components (such as Protocol) appear, enter the requirements according to the instructions of your network administrator.
12. Restart Windows NT.



➤ **To uninstall the SA-PCR drivers in Windows NT:**

- 1.** From the Windows *Start* menu, select **Settings**, and then select **Control Panel**. Double click the **Network** icon, click the **Configuration** tab, select **BreezeNET Wireless LAN PC card**, and click **Remove**.
- 2.** Insert the BreezeCOM Drivers diskette. From the Windows *Start* menu, select **Run**, and type a:\DrvClean.
- 3.** When notified that the SA-PCR driver has been deleted, click **Setup**.
- 4.** Restart the computer.


## **Installing the SA-PCR Drivers in Windows CE**

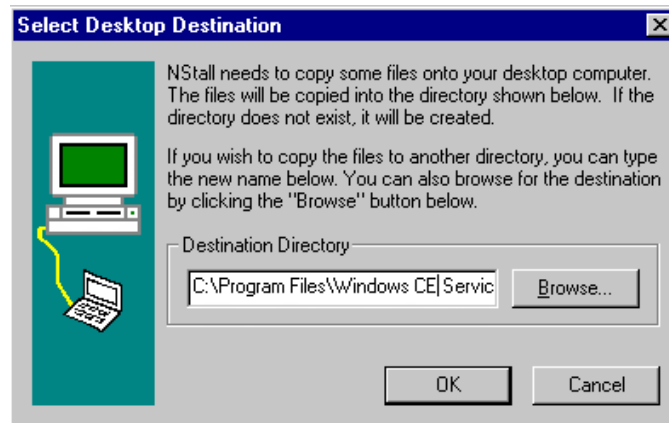
When installing the SA-PCR drivers on handheld PCs (H-PC), you must first connect the H-PC to its host desktop PC and establish a connection between them.

- 1.** Connect the H-PC to COM port 1 or 2 of the host desktop PC, using an RS-232 serial cable.
- 2.** Insert the Windows CE Service application CD into the CD drive of the host desktop PC. The application setup program is automatically displayed. If it is not displayed for any reason, double-click the **setup.exe** file from the CD folder.
- 3.** Follow the on-screen instructions of the setup program.
- 4.** Check that the Baud Rate of the desktop PC and the H-PC are identical (the default is 19200 bps). Continue to Step 5.  
If the Baud Rate is not identical in both PCs, follow the instructions below to change the *Baud Rate* on the H-PC:
  1. Click the **My handheld PC** icon.
  2. Double-click the **Control Panel** icon and select **Communications and Properties>PC Connection** tab.
  3. Click the **Change** button.

4. From the dropdown list, select the baud rate that matches the baud rate of the PC.
5. Click **OK**.
- 5.** After changing the configuration of the H-PC, reset the device by pushing in the **Reset** button of the H-PC (usually located at the bottom of the PC).
- 6.** Double-click the **setup.exe** file. After the introductory notice, the following window is displayed.



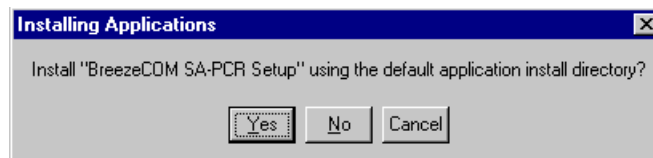
7. Click the  button to begin the installation process.





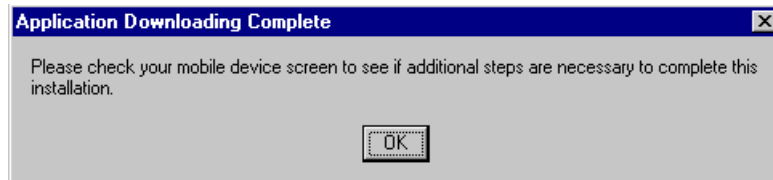
8. Choose the installation destination folder (C:\Program Files\Windows CE Services by default).



9. Click **OK**.



- 10.** Click  to install the application in the Windows CE directory of the H-PC. Click  to install the application in a different directory. The setup program copies files from the desktop PC the H-PC. The progress bar, briefly displayed on the screen, indicates the completion of this process.



- 11.** Check your mobile device screen for any additional steps required to complete the installation process. For example, replacing an old version of the driver (if you have one installed) with a new version. If you need to perform additional installation steps, follow the instructions on the mobile device screen. If no additional steps are needed, click **OK** to complete the installation.
- 12.** Insert the SA-PCR card in a free PCMCIA slot of the H-PC.

## Checking the LED Indicators

Verify correct operation of the SA-PCR using the following LED indicators table:

**Table 4-1: SA-PCR Card LED Indications**

Color	Description	Meaning
Yellow	Link Status	Blink – Scanning
		Solid – Associated
Green	Data Traffic	Blink – According to traffic

The LED indicators are useful only if there is an active AP in the area.

The LED indicators can be used to verify correct firmware download procedures; the LEDs turn on and off quickly, one LED being ON while the other is OFF.

## Initial Configuration

If your wireless network uses a non-default ESSID, enter the required ESSID as follows:

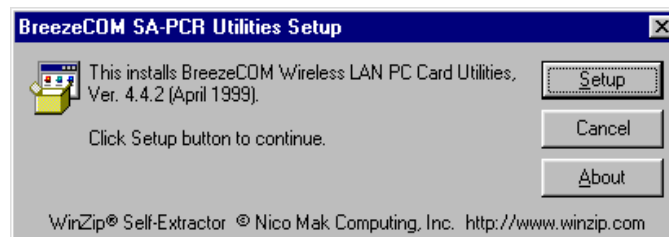
1. Start the Configuration Utility by, from the Windows *Start* menu, selecting **Programs**, then **BreezeCOM Utilities**, and then **Configure**.
2. Edit the **ESSID** parameter by clicking the *WLAN Parameters* tab and entering the ESSID that matches the AP unit.
3. Restart the computer.

## Installing the SA-PCR Utilities

If a previous version of the SA-PCR utilities is installed, uninstall it before reinstalling the new version.

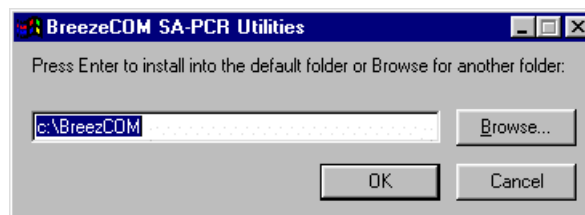
➤ **To install the SA-PCR utilities:**

1. Insert the BreezeCOM Utilities diskette.
2. From the Windows *Start* menu, select **Run**. Type A:\setup, and click **OK**.
3. When the notification window is displayed; click **Setup**.



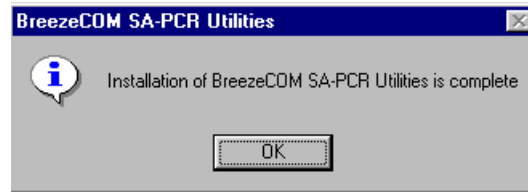
**Figure 4-6: BreezeCOM SA-PCR Utilities Setup**

4. In the *BreezeCOM SA-PCR Utilities* window, navigate to the required installation location and click **OK**.



**Figure 4-7: BreezeCOM SA-PCR Utilities - Folder Selection Window**

5. When the *BreezeCOM SA-PCR Utilities Setup Complete* window is displayed, click **OK**. Icons for the utilities are added to the Windows *Programs* menu, and an SA-PCR Configure icon is added to the *Control Panel*.



**Figure 4-8: BreezeCOM SA-PCR Utilities Setup Complete Window**

## Installing the SA-PCR Driver for Windows 2000 Systems

This section describes the software installation of the SA-PCR station adapter in PCs running the Windows 2000 operating system.


To perform this procedure, you will need the driver kit, which consists of the BRZW2KA.EXE file. Running this file installs both the SA-PCR driver and the BreezeNET Configuration utility (a Windows Control Panel applet). You can download the driver kit from [www.alvarion.com](http://www.alvarion.com). Call Alvarion customer support for further information.

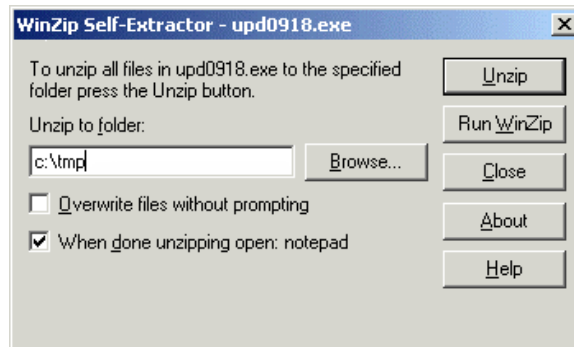
When installing certain models of the card with Windows 2000, the system automatically installs the SA-PCR driver from the Microsoft Windows 2000 Installation CD. This driver has restricted capabilities and is not compatible with some BreezeNET features (such as the Configuration utility). To install a driver that is fully compatible with all BreezeNET features, perform the upgrade procedure described in *Upgrading the Windows 2000 Driver for PnP SA-PCR*, on page 4-26.

## Installing the Windows 2000 Driver Kit

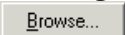
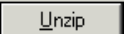
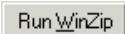
Installing the SA-PCR Driver for Windows 2000 requires the Windows 2000 Driver kit

➤ **To install the Windows 2000 Driver Kit:**

1. Run the BRZW2KA.EXE file. Click  when prompted. The following window is displayed.



**Figure 4-9: Installing the Windows 2000 Driver Kit**

2. By default, the driver kit program extracts the files to the TMP directory of your default hard drive. To change the location, enter the path in the *Unzip to folder* field or click  and navigate to the directory of your choice.
3. Click  to start extracting, or click  to open the Winzip application if you need to control the extraction process. After extraction, a message is displayed informing you that the files were extracted.



## Installing SA-PCR Cards With Windows 2000

This section describes how to install SA-PCR cards on PCs running Windows 2000.

### ➤ To install the SA-PCR Cards With Windows 2000:

1. Physically install the SA-PCR card.
2. Start the PC and login to the system with Administrator access rights. A *Found New Hardware* message is displayed.
3. Follow the instructions provided by the *Add Hardware Wizard* and when prompted, navigate to the driver file installed by BRZW2KA.EXE (located in C:\TMP by default).



#### NOTE:

If Windows 2000 does not ask you to specify the location of the driver and installs one automatically from the Windows 2000 CD, perform the procedure in *Upgrading the Windows 2000 Driver for PnP SA-PCR*, on page 4-26.

If Windows displays the *Digital Signature Not Found* message, click **Yes**. This update may contain drivers that are not digitally signed.

After the driver installation is complete, open the Configuration Utility and select the required ESSID and country code.

If you do not need to restart Windows, eject the card and insert it again. The device will now operate with the updated driver. The new settings become effective after the card is removed and inserted again, or Windows is restarted.




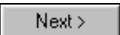



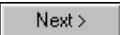


#### IMPORTANT:

Before removing the card, be sure to perform the Stop function from the Removable devices Taskbar icon. This icon is normally visible if removable devices are attached to your PC. Removal of a device without stopping it first can crash Windows and cause the loss of your data.

## Upgrading the Windows 2000 Driver for PnP SA-PCR Cards

If Windows 2000 automatically installed the SA-PCR driver on the Microsoft Windows 2000 Installation CD, you will need to perform the following upgrade procedure. The driver provided on the Windows 2000 Installation CD has restricted capabilities and is not compatible with some of the BreezeNET features (such as the Configuration utility).

1. Open the Device Manager with Administrator access rights (if you have not logged in as an Administrator).
2. Expand the Network Adapters branch and select the **BreezeNET Wireless LAN PC Card**.
3. Click  and select the *Driver* tab of the *Properties* window.
4. Click . The *Update Device Driver Wizard* starts. Click .
5. Select the **Display a list of all drivers...** option and click .
6. Click .
7. Enter the location path and name of the driver or browse to the location where the driver can be found (C:\TMP by default). A list appears containing exactly one item. Select it and click . Then click .
8. In the *Wizard is ready to install...* window click . If Windows displays the *Digital Signature Not Found* message, click **Yes**. This update may contain drivers that are not digitally signed.
9. Click **Finish**.
10. After the driver update is complete, open the Configuration Utility from the Control Panel by selecting **Settings** from the Windows *Start* menu and then selecting **Control Panel**. Double click the **BreezeCOM Configuration** icon.

11. Select the required ESSID and country code.



**NOTE:**

If Windows prompts to restart, click **YES** and restart Windows; while Windows is shut down, remove the card (so you can use the Configuration Utility before the card starts).

12. If you do not need to restart Windows, eject the card and insert it again. The new settings became effective after the card is removed and inserted again, or Windows is restarted.



**IMPORTANT:**

If Windows prompts to restart, click YES and restart Windows; while Windows is shut down, remove the card (so you can use the Configuration Utility before the card starts). Before removing the card, be sure to perform the Stop function from the Removable devices Taskbar icon. This icon is normally visible if removable devices are attached to your PC. Removal of a device without stopping it first can crash Windows and cause loss of your data.

## Installing/Updating the Site Survey

The Site Survey utility can be installed and updated as a separate package. Users do not need Administrator rights in order to install and run it.



**NOTE:**

Do not use the Win9x Site Survey utility with Windows 2000; only use the Windows 2000 Site Survey utility.

To install the Site Survey application, run the SURVEY.EXE file installed by BRZW2KA.EXE (located in C:\TMP by default).

➤ **To uninstall the SA-PCR utilities:**

1. From the Windows *Start* menu, select **Programs**, select **BreezeCOM Utilities** and then select **Uninstall**.
2. You can also uninstall the SA-PCR utilities by using the Windows Add/Remove Programs feature.

# Using the SA-PCR Configuration Utility

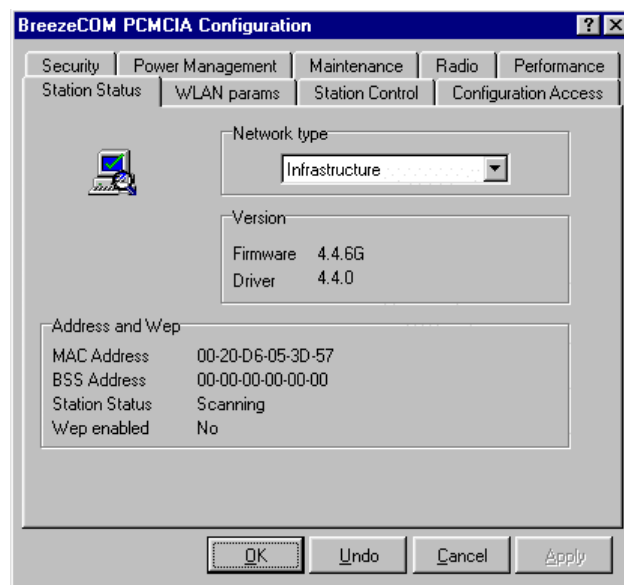
**NOTE:**

If you are using a Windows CE device, refer to page 4-42.

This section describes how to use the SA-PCR Configuration utility to configure and manage your SA-PCR card.

Access the SA-PCR Configuration utility as follows: From the Windows *Start* menu, select **Programs**, select the **BreezeCOM Utilities** program group and then select **Configure**.

The *BreezeCOM PCMCIA Configuration* window is displayed as follows, with the *Station Status* tab selected.



**Figure 4-10: SA-PCR Configuration Utility Main Window - Station Status Tab**

The *BreezeCOM PCMCIA Configuration* window contains several tabs, as described in the following sections.

In addition, the configuration windows contain the following buttons:

- ◆ **OK:** Implements any changes and closes the window.
- ◆ **Undo:** Causes the window to display currently active values. This is useful if you started changing values and must start again from the current values.
- ◆ **Cancel:** Closes the window without implementing any changes
- ◆ **Apply:** Implements any changes while leaving the window open.

## Station Status Tab

The *Station Status* tab of the SA-PCR Configuration utility displays information regarding the card and the card's status.

The **Station Status** tab contains the following parameters:

- ◆ **Network Type:** In the current version, the value of this parameter should be always set to Infrastructure.
- ◆ **Firmware Version:** Displays the version of unit's current firmware (internally installed software). The first two numbers of the firmware and driver versions should be identical. The remaining numbers (if any) indicate the minor version. The final letter indicates the hardware version.
- ◆ **Driver Version:** Displays the version of unit's current driver.
- ◆ **MAC Address:** Displays the unit's unique IEEE MAC address.
- ◆ **BSS Address:** The MAC address of the AP with which the unit is currently associated.
- ◆ **Station Status:** Current status of the unit. There are two possible options:

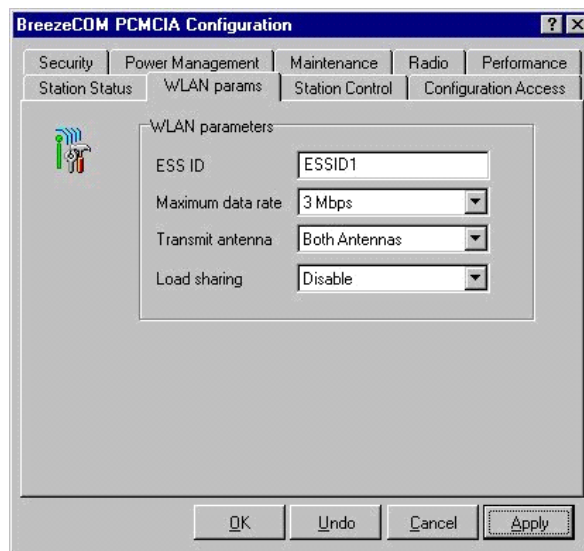
- ❖ **Scanning:** The unit is searching for an AP with which to associate.
- ❖ **Associated:** The unit is associated with an AP and has adopted the attached PC MAC address.
- ♦ **Wep enabled:** Wired Equivalent Privacy (WEP) is an authentication algorithm that protects authorized Wireless LAN users against eavesdropping. The definition of WEP is well defined in the 802.11 standard.

**NOTE:**

Parameter changes take effect only after reset.

## WLAN Parameters Tab

The *WLAN Parameters* tab of the SA-PCR Configuration utility enables you to view and edit basic Wireless LAN parameters of the card.



**Figure 4-11: WLAN Parameters Tab**

The *WLAN Parameters* tab contains the following parameters:

- ◆ **ESSID:** An ASCII string of up to 32 characters used to identify a WLAN that prevents the unintentional merging of two co-located WLANs. It is essential that the ESSID is set to the same value in all stations and Access Points in the extended WLAN. The ESSID field is case-sensitive.
- ◆ **Maximum Data Rate:** By default, the unit adaptively selects the highest possible rate for transmission. Under certain conditions (for range/speed trade-off) you may decide not to use the higher rates. Possible values are **1**, **2**, or **3Mbps**.
- ◆ **Transmit Antenna:** By default, the unit dynamically selects the antenna where reception and transmission is optimal. If your model has an external antenna and uses only a single antenna, set the **Transmit Antenna** to transmit only from that single antenna. Antenna number one is the antenna nearest the yellow LED.
- ◆ **Load Sharing:** When installing a Wireless LAN network in a high-traffic environment, you can increase the aggregate throughput by installing multiple APs to create co-located cells. Enable **Load Sharing** to cause your stations to equally divide their traffic between the available APs.

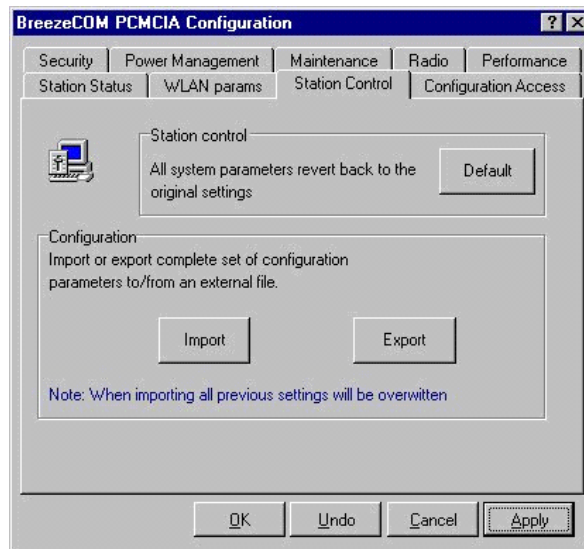


**NOTE:**

Parameter changes take effect only after reset.

## Station Control Tab

The *Station Control* tab of the SA-PCR Configuration utility enables you to return the card to default configuration values, and export/import configuration files.



**Figure 4-12: Station Control Tab**

The *Station Control* tab contains the **Default** button which reverts all parameters to factory default values.

As a time saving feature, you can configure one unit and then save the configuration as a file (with a.BRZ extension). You can later import the configuration file to other units.

- ◆ **Import:** Imports a configuration file to this unit, and overwrites all previous settings.
- ◆ **Export:** Exports the current configuration of this unit to a file.



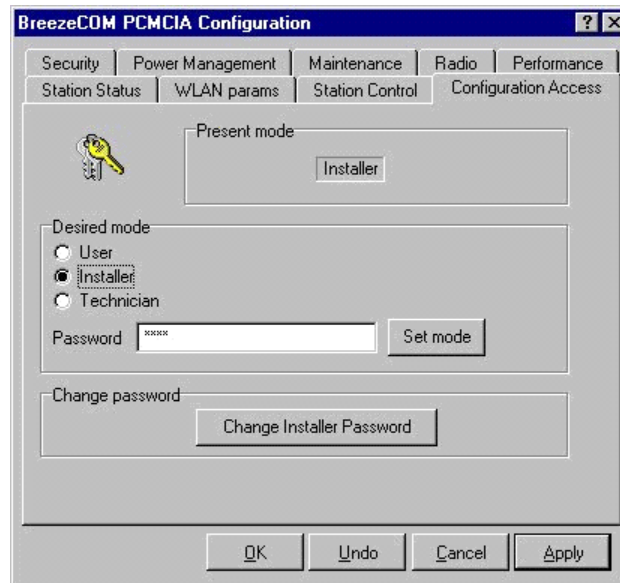


**NOTE:**

Parameter changes take effect only after reset.

## Configuration Access Tab

The *Configuration Access* tab of the SA-PCR Configuration utility enables you to login to the card as User, Installer, or Technician, and enables you to change the password.



**Figure 4-13: Configuration Access Tab**

The *Configuration Access* tab displays the current mode (User, Installer, or Technician) in the **Present Mode** box. This mode determines the security access to system parameters. Users can view some of the window tabs, but cannot modify parameters. Installers can view all of the tabs and can modify some of the values. Technician access rights are reserved for certified Alvarion technicians.

When the Configuration utility opens, it starts at the same mode that was active when it closed. If security is an issue, change the access mode to User before you close the utility. The first time the utility is opened, it is set to Installer access mode.

The default password for Installer mode is User, however you can change this password if security considerations play an important role in the construction of your WLAN.

➤ **To change the Configuration Access mode:**

1. Select the radio button next to the desired mode.
2. Type in the password. No password is necessary to lower the access right level.
3. Click **Set mode**. The name of the new mode appears in the **Present Mode** box.

➤ **To change the password for Installer Configuration Access mode:**

1. Look at the **Present Mode** box to verify that you are in Installer mode.
2. Click **Change Password**.
3. In the *Change Password* window, type in the new password twice and click **OK**. The BreezeNET Monitor changes your password.



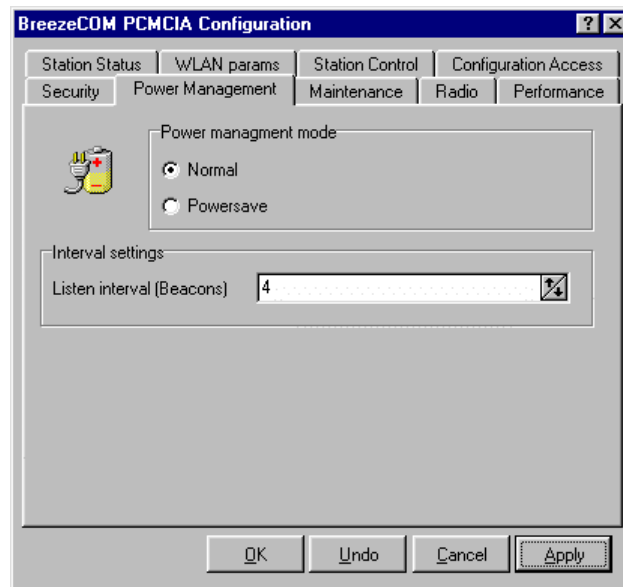
**NOTE:**

If the Installer password is misplaced you will be unable to change the unit's access rights.

## Power Management Tab

The **Power Management** tab of the SA-PCR Configuration utility enables you to enable/disable Power Save mode and to configure Power Save mode parameters.

Power Save mode is intended for laptops or hand-held computers to conserve battery energy. When Power Save mode is enabled, the unit “sleeps” most of the time and “wakes up” occasionally to transmit/receive to/from the AP. This extends the battery life span of a laptop installed with the SA-PCR.



**Figure 4-14: Power Management Tab**



**NOTE:**

Expect a degradation in performance of the entire cell, even if only the AP and one station are set to Power Save mode.

The *Power Management* tab includes the following parameters:

- ♦ **Power Management Mode:** Enable Power Save mode by clicking the **Powersave** option; disable by clicking the **Normal** option (default).

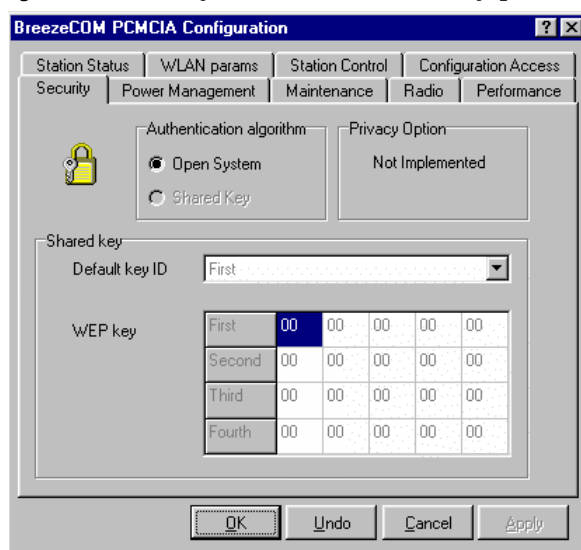
- ◆ **Listen Interval Settings:** Specifies how often the station is to “wake up” to transmit or receive data (unicast packets). This parameter enables performance optimization on a per station basis. In contrast, the DTIM period (that is set in the AP only) defines the time period for **all** stations in the cell to “wake up” in order to receive broadcasts.

**NOTE:**

If the Power Save mode is enabled on one of the WLAN's SA-PCR stations, you must also enable the Power Save mode on the AP through the BreezeNET monitor. Refer to *Performance*, on page 3-26 for further information.

## Security Tab

The *Security* tab enables you to set the security parameters of the station.



**Figure 4-15: The Security Tab**

The station in which the SA-PCR card is installed can use one of the following authentication algorithms (as defined in the 802.11 standard).

- ♦ **Open System:** Any station in the WLAN can associate with an AP and receive and transmit data (no authentication).
- ♦ **Shared Key:** Only stations using a shared key encryption identified by the AP are allowed to associate with it. You can only select this option if the card was ordered with the Privacy option or if you enabled the WEP feature during the upgrade procedure. To see whether the WEP option was enabled during installation, select the *Station Status* tab.

<b>Values:</b>	Unknown	Card is not inserted.
	Implemented	Shared Key authentication is enabled.
	Not Implemented	Shared Key authentication is disabled. Only open system authentication is available in this mode.

If you selected the Shared Key algorithm, proceed to configure the following parameters:

- ♦ **Default Key ID:** Sets the default key for encryption in the Authentication process. This is the encryption key that is used for transmissions between the station and the AP.
- ♦ **WEP Key:** Define the encryption keys used for transmissions between the station and the AP. Specify each key by clicking the appropriate WEP Key row (First, Second, Third or Fourth) and entering 10 hexadecimal digits (5 pairs of characters) for each of the 4 keys.

To configure security parameters in ODI/DOS environment, use the *brzsetup* application.



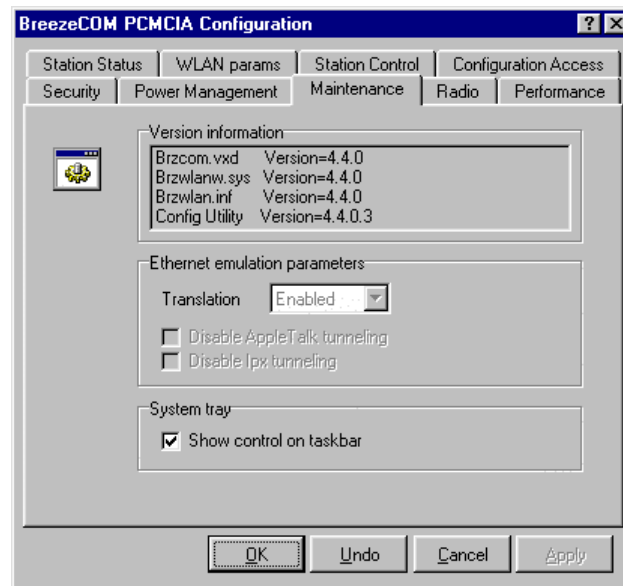
#### NOTES:

The default Key ID you enter for the SA-PCR must match the Key ID defined in the AP. *Security*, on page 3-22, describes the procedure for setting the encryption keys for BreezeNET APs. It is recommended to change the encryption keys periodically, to enhance system security.

## Maintenance Tab



The *Maintenance* tab of the SA-PCR Configuration utility enables you to cause the unit to verify firmware/driver compatibility, and set how the unit handles 802.3 packets.

This tab is not visible in User login mode. When in Installer mode, the parameters are read-only. When in Technician mode, the parameters can be edited.



**Figure 4-16: Maintenance Tab**

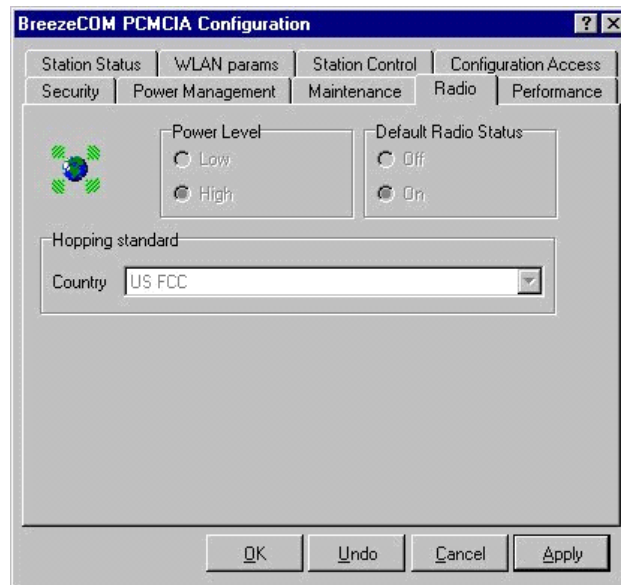
The *Maintenance* tab contains the following parameters:

- ◆ **Version Information:** Windows drivers are divided into three files: Brzcom.vxd, Brzwlanw.sys, and Brzwlan.inf. The version number of all these files must be identical. Control information of these files is displayed. The Configuration utility file is called BrzConfig.exe. The first two numbers of the Configuration utility version must match the first two numbers of the drivers.
- ◆ **Disable AppleTalk tunneling:** Enables you to disable (default) or enable AppleTalk tunneling if the network contains a mix of Ethertalk 1 (ET 1) and Ethertalk 2 (ET 2) stations to ensure smooth communications. Ensure that all units are set to the same tunneling settings.
- ◆ **Show control on taskbar:** Check this box to display the  icon on the Windows taskbar. When this option is enabled, you can double click the  icon to display the SA-PCR Configuration utility at any time.

## Radio Tab

The *Radio* tab of the SA-PCR Configuration utility enables you to set the power level of the unit and choose a hopping standard.

This tab is not visible when in User mode. When in Installer mode, you can the parameters are read-only. When in Technician mode, the parameters can be edited.



**Figure 4-17: Radio Tab**

The *Radio* tab contains the following parameters:

- ◆ **Power Level:** Level of power at which the unit is operating. There are two possible options: **Low** or **High**.
- ◆ **Default Radio Status:** When **On** the radio receives in regular mode. When **Off** the radio does not work at startup. For example, when traveling in planes.



- ♦ **Hopping Standard:** A set of rules regarding the radio transmission standard allowed in each country. Units work together only if set to the same hopping standard. Use this parameter to set the unit's hopping standard to that of the relevant country. Proprietary hopping standards can also be implemented. Refer to *Radio*, on page 3-28.

## Performance Tab

The *Performance* tab of the SA-PCR Configuration utility enables you to fine-tune performance and roaming parameters. This tab is not visible when in User mode. When in Installer mode, the parameters are read-only. When in Technician mode, the parameters can be edited. Only major parameters are described below.



### NOTE:

All fields in this window are read only.

The screenshot shows the 'BreezeCOM PCMCIA Configuration' window with the 'Performance' tab selected. The window has a title bar with a question mark and a close button. Below the title bar are several tabs: 'Station Status', 'WLAN params', 'Station Control', 'Configuration Access', 'Security', 'Power Management', 'Maintenance', 'Radio', and 'Performance'. The 'Performance' tab is active, showing two sections: 'Performance' and 'Roaming'. The 'Performance' section includes a red clock icon and four parameters: 'Rts threshold (Bytes)' set to 1600, 'Maximum retransmissions' set to 1, 'Dwells to retransmit' set to 2, and 'Multirate support' set to 'Enable'. The 'Roaming' section includes five parameters: 'Joining window' set to 1, 'Leaving threshold (dBm)' set to -77, 'Joining threshold (dBm)' set to -72, 'Num of beacons to disconnect' set to 7, and 'Neighbor aging time (Sec)' set to 20. At the bottom of the window are four buttons: 'OK', 'Undo', 'Cancel', and 'Apply'.

Section	Parameter	Value
Performance	Rts threshold (Bytes)	1600
	Maximum retransmissions	1
	Dwells to retransmit	2
	Multirate support	Enable
Roaming	Joining window	1
	Leaving threshold (dBm)	-77
	Joining threshold (dBm)	-72
	Num of beacons to disconnect	7
	Neighbor aging time (Sec)	20

**Figure 4-18: Performance Tab**

The *Performance* tab contains the following parameter:

- ◆ **Rts threshold (bytes):** Minimum packet size to require an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the WLAN.

## Resetting the SA-PCR Card

It is necessary to reset the SA-PCR card after making configuration changes via the SA-PCR Configuration utility. Perform this procedure as follows:

1. Close the Configuration and Site Survey utilities and then complete one of the following:
  - ◆ Restart the computer, OR
  - ◆ Stop the PC card then eject and reinsert the card, OR
  - ◆ Stop and refresh the driver as follows:
2. Right-click the **My Computer** icon on the desktop, select **Properties**, and then select the *Device Manager* tab.
3. Select **Network Adapters**, then select **BreezeNET WLAN PC Card**, and click **Refresh**.

## Running the Configuration Utility with Windows 2000

The Configuration Utility is located in the Control Panel. Windows Administrators have Installer user rights by default. Other users have User access rights by default, and normally can not change the settings. This is part of Windows NT system protection policy.

In order to use the Configuration Utility when you are not logged on as an Administrator, you can create a shortcut to BRZWLAN.CPL in the *All Users' Programs* menu or another folder.

In the *Properties* page of this shortcut, check **Run as different user**. You must enter the Administrator password to run it as Administrator.

Additional general comments on the Configuration utility:

- ◆ When the card can not establish a link with an Access Point (the yellow LED blinks), the Taskbar icon will indicate *Network cable unplugged*. Wireless Ethernet devices report their unconnected state as their cable being unplugged. This is a feature of Windows 2000.
- ◆ This update removes the *Advanced* tab on the device properties; the configuration can only be completed using the Configuration utility.
- ◆ In the event that the driver does not work properly after performing the driver upgrade or when changing the configuration, you may need to reset parameters to factory default using the updated Configuration utility; then re-apply the required parameters.
- ◆ The Device Manager will not display non-present plug-and-play devices, even when the **Show hidden devices** option is active.
- ◆ In order to access the driver in Device Manager without inserting the card, start Windows 2000 in Safe mode, or set the environment variable:

DEVMGR\_SHOW\_NONPRESENT\_DEVICES=1

## Troubleshooting Tips

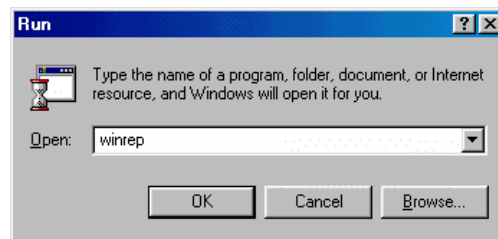
To perform the troubleshooting procedures described here, the user is required to have knowledge of Windows NT procedures, such as using the event log, and machine administration.

### ***Make sure that your machine has an updated BIOS***

The PCMCIA/Cardbus controller must be properly initialized by BIOS in order to work with Windows 2000. Even machines listed as Windows 2000 compatible may still have an outdated BIOS. In case of strange resource allocation problems, check the BIOS.

### ***Use the Winrep utility to create your problem report***

From the Windows *Start* menu, select **Run**. Type Winrep.



Allow Winrep to collect system information. Check the Event log for relevant messages.

Using the Event Viewer's Copy command, paste the message into your report or save the entire System log as an attachment.

In case of a *blue screen*, copy the error code that is displayed. You can also select a small memory dump in System Properties, Startup and recovery... Write debugging information... Small memory dump. The small dump file contains all information from the *blue screen*. Attach this dump file to your report.

Save the report to file and send it to Technical Support.



#### **IMPORTANT:**

Data collected by Winrep contains your user name and other information that you may consider sensitive.

# Using the Windows CE SA-PCR Utility

The Windows CE version of the SA-PCR software includes two tabs:

- ◆ **Configuration**
- ◆ **Monitor**

➤ **To open the software:**

- 1.** Click the SA-PCR icon located at the bottom right hand corner of the H-PC Status bar.
- 2.** Click either the *Configuration* tab or the *Monitor* tab.

## Configuration

The *Configuration* tab includes the following parameters:

- ◆ **ESSID:** An ASCII string of up to 32 characters used to identify a WLAN that prevents the unintentional merging of two co-located WLANs. It is essential that the ESSID be set to the same value in all stations and Access Points in the extended WLAN. The ESSID field is case-sensitive.
- ◆ **Rate:** By default, the unit adaptively selects the highest possible rate for transmission. With certain conditions (for range/speed trade-off) you may decide not to use the higher rates. Possible values are **1**, **2**, or **3Mbps**.

- ◆ **Power Level:** Level of power at which the unit is operating. There are two possible options: **Low** or **High**.
- ◆ **Power (Power Save):** Enable the Power Save mode by clicking the **Powersave** option; disable the option by clicking the **Normal** option (default).

**NOTE:**

If the Power Save mode is enabled on one of the WLAN's SA-PCR stations, you must also enable the Power Save mode on the AP through the BreezeNET monitor. Refer to the *Performance*, on page 3-26 for more information.

- ◆ To apply the new configuration, click **Update**. After changing the configuration you must reset the SA-PCR card by pulling it out of the H-PC and –re-inserting it.

**NOTE:**

To obtain full access to the configuration parameters, use the Configuration utility available from Alvarion authorized dealers.

## Monitor

The *Monitor* tab includes the following parameters:

- ◆ **Driver Version:** The current driver version installed on the mobile device.
- ◆ **Firmware Version:** The current installed firmware version.
- ◆ **H/W Version:** The current hardware version of the inserted card.
- ◆ **SA-PCR:** The MAC address of the SA-PCR card.
- ◆ **Current BSSID:** The MAC address of the current AP.
- ◆ **Current RSSI Level:** The current RSSI readouts of the station.

- ◆ **Station Status:** Current status of the unit. There are five options:
  - ❖ **None:** No association with an AP (the station is scanning for an AP with which to associate).
  - ❖ **Synchronized:** The station is synchronized with an AP but has not yet learned its WLAN MAC address.
  - ❖ **Authenticated:** The card has been identified by the AP and is allowed to access the network.
  - ❖ **Associated:** The station is associated with an AP and has adopted the attached PC MAC address.
  - ❖ **Roaming**

# Using the SA-PCR Site Survey Utility

**NOTE:**

This utility can not be used in systems installed with ODI.

This section describes how to use the SA-PCR Site Survey utility to manage your SA-PCR card. The Site Survey utility keeps you informed of the signal strength at which your unit is receiving.

You can run a Site Survey to compare reception at various locations. This is extremely useful when first setting up the wireless LAN, since you can easily determine where reception is good or bad, and where many Access Points overlap.

The following sections describe how to access the Site Survey utility, how to read the main Site Survey window, and how to perform a site survey.



## Accessing the SA-PCR Site Survey Utility

Open the SA-PCR Site Survey utility as follows: From the Windows *Start* menu, select **Programs**, select the **BreezeCOM Utilities** program group and then select **Site Survey**. The *BreezeCOM Site Survey* window is displayed.

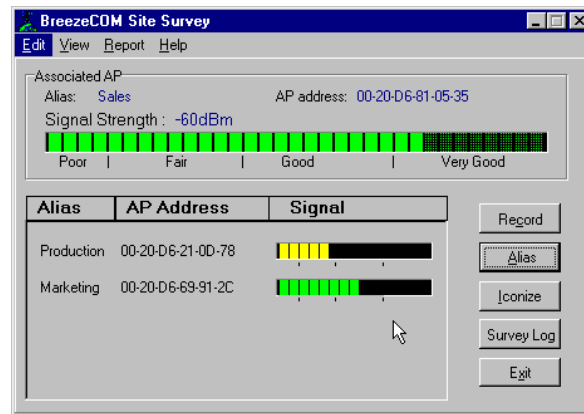


Figure 4-19: SA-PCR Site Survey

## SA-PCR Site Survey Main Window

The main Site Survey window contains the following sections:

- ♦ **Associated AP:** This section, located at the top of the window, displays various parameters regarding the Access Point with which the unit is currently associated.
- ♦ **Alias:** The alias you have assigned to the AP with which the SA-PCR is currently associated. To assign aliases to AP units, click **Alias**. If no alias has been assigned to the AP, this field displays “no alias”.
- ♦ **AP Address:** The IEEE MAC address of the AP.

- ♦ **Signal Strength:** The strength of the signal from the AP in dBm. The table below maps the signal strength indicators to dBm ranges:

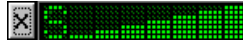
Signal	Poor	Fair	Good	Very Good
dBm	less than -74	-74 to -69	-68 to -61	greater than -61

- ♦ **Signal Bar:** The signal bar is a graphical representation of the signal strength. The longer the bar, the stronger the signal. As signal strength drops, the bar changes from green, to yellow, to red
- ♦ **Neighbor APs:** This section, located at the bottom of the window, displays nearby APs (up to 4) from which the station is receiving a signal. For each AP, the following parameters are displayed:
  - ❖ **Alias:** The alias assigned to the AP. To assign aliases to AP units, click **Alias**. If no alias has been assigned to the AP, this field displays “no alias”.
  - ❖ **AP Address:** The IEEE MAC address of the AP.
  - ❖ **Signal:** A miniature signal bar indicating the current signal strength from the AP. When you hold the cursor over the line, the exact value is displayed.

The following buttons appear on the right side of the main Site Survey window. Several of the buttons are used in the course of performing a Site Survey.

- ♦ **Record:** Records the signal strength of the current location in the Survey Log, as well as all neighboring APs. In the *Record* window, you can add the name of the location and a remark. You can view the Survey Log by clicking **Survey Log**.
- ♦ **Alias:** Enables you to assign alias names to APs. In the *Alias* window, enter the AP address and the required alias. For convenience, you can drag and drop the address of the associated AP from the main window into the *Alias* window. For neighbor APs, you should use Ctrl-C to copy the AP address from the main window.

- ♦ **Iconize:** Closes the *Site Survey* window and opens the *Connection Quality Graph* that indicates current signal strength of the associated AP at a glance. The Graph can be moved anywhere on the screen, and always appears on top of other applications. Hold the cursor over the X to see the signal strength in units. Click the X to close the Graph and open the Site Survey window.



**Figure 4-20: Connection Quality Graph**

- ♦ **Survey Log:** Opens the *Survey Log* at the bottom of the main window. The *Survey Log* displays the information recorded using the **Record** button. Click **Clear Log** to clear the *Survey Log*. Click **Delete Last** to delete the last recorded reading.

Survey Location	Associated AP	Signal	Remark
Here	AP#13	112	With Antennas
There	AP#13	203	With Antennas
Near by	AP#13	85	without antennas

**Figure 4-21: Survey Log**

- ♦ **Menu Bar:** The menu bar at the top of the window contains four menus - *Edit*, *View*, *Report* and *Help*. These menus contain sub-menus which correspond in most cases to the buttons at the side of the window.
  - ❖ **Edit Menu:** Comprises three sub-menus, *Record*, *Alias* and *Exit*.
  - ❖ **View Menu:** Comprises two sub-menus, *Survey Log* and *Iconize*.

- ❖ **Report Menu:** Comprises two sub-menus: *Preview* and *Print* (do not have corresponding buttons on side of window).
  - ◆ **Preview:** Enables you to preview a site survey report before proceeding further.
  - ◆ **Print:** Opens a Site Survey report showing the information in the *Survey Log*, including neighboring APs.  
You can print the file by clicking the **Printer** button, or save the file by clicking the **Diskette** button. You can save the file as text, or as a QRP file viewable using this application.
- ❖ **Help Menu:** Comprises two sub-menus, *About* and *Getting Started* (do not have corresponding buttons on side of window).
  - ◆ **About:** Contains standard Windows format information about the application.
  - ◆ **Getting Started:** Provides basic information to enable you to begin working.

## Performing a Site Survey with the SA-PCR

You can run a Site Survey to compare reception at various locations. This is extremely useful when first setting up the wireless LAN, since you can easily determine where reception is good or bad, and where many Access Points overlap.

### ➤ To run a Site Survey:

1. Open the Site Survey utility.
2. Click **Survey Log** to expand the bottom of the Site Survey window.
3. Bring the station to a new location.
4. Click **Record**. Type in the name of the location and a remark, and click **OK**. The signal details of the current location appear in the Survey Log at the bottom of the window.

5. Repeat steps 2 and 3 with other locations. The recorded readings should give you a good idea of where reception is good or bad, and where many APs overlap unnecessarily.
6. When you are done recording, click **Print**. A site survey report is displayed containing information about each recorded location including signal strength of associated AP and of neighbor APs. You can print the file by clicking the **Print** button, or save the file by clicking the **Diskette** button. You can save the file as text, or as a QRP file, which can be viewed using this application only.

## Using the Upgrade Kit Program

The Upgrade kit program is an application that enables you to upgrade previous versions of the firmware, drivers and utilities of the SAPCR, if installing on a machine that had a previous version. The Upgrade kit can be obtained from the Alvarion Web site.

In addition, with Windows 95/98 you can use this program as another way to install the firmware, driver and utilities.

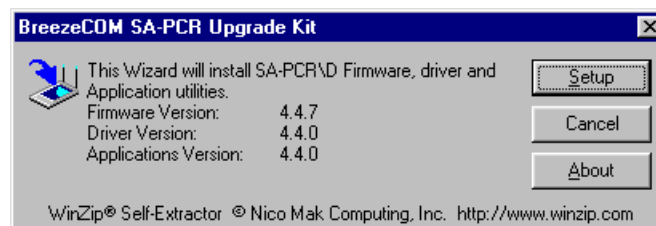
**NOTE:**

Upgrading causes your system to lose all configuration parameters that were previously set.

### Upgrade Procedure for Windows 95/98

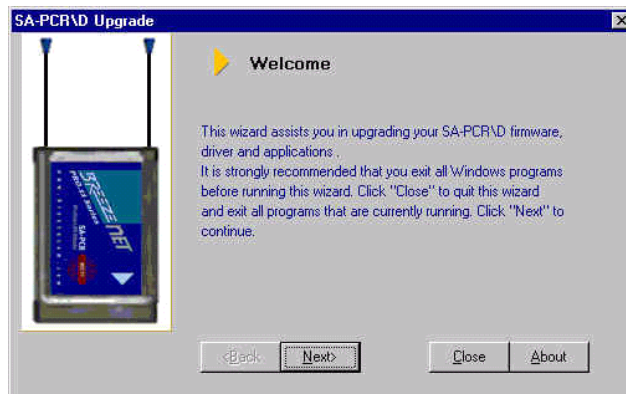
This section describes how to upgrade on a PC running Windows 95/98.

1. Run the UPGR4402.EXE program from the diskette. The following window is displayed.



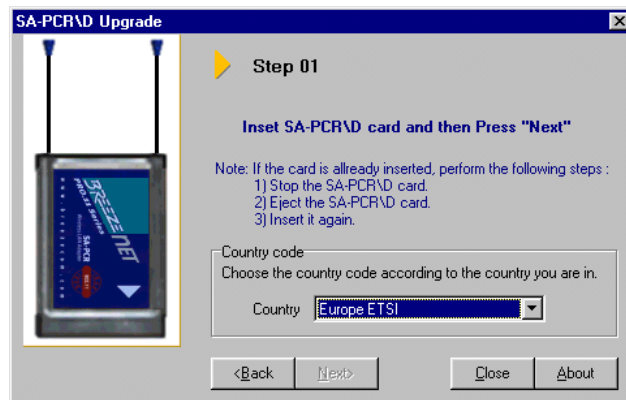
**Figure 4-22: Upgrade Kit Program Introductory Window**

2. Click **Setup**. The following window is displayed.



**Figure 4-23: Upgrade Kit Program Welcome Window**

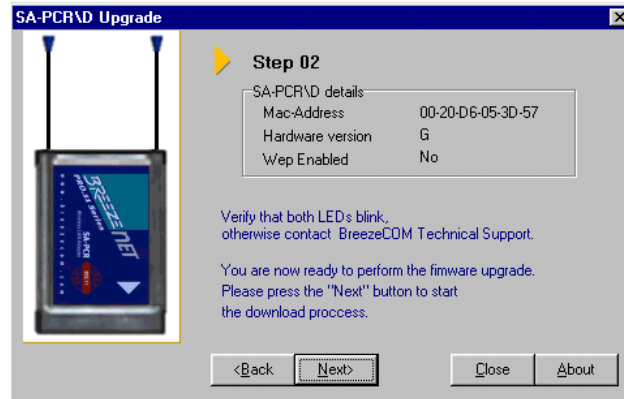
3. Click **Next**. The following window is displayed.



**Figure 4-24: Upgrade Kit Program Step 1**

4. From the **Country** dropdown list, select the standard applicable to your country and click **Next**. You do not need to select the country if you are installing the application in the following countries: USA/FCC, Europe/ETSI or Japan.

5. If the card is already installed, stop the card as follows: From the *Control Panel*, double click the **PCMCIA Card** icon, select the BreezeCOM card and click **Stop**. Remove the SA-PCR card from the slot. Wait for about 15 seconds and then reinsert. Click **Next**.



**Figure 4-25: Upgrade Kit Program Step 2**

The MAC address of the PC and the hardware version of the SA-PCR card are displayed in read-only field.



6. If you purchased the SA-PCR without the Wired Equivalent Privacy (WEP) feature and you require this feature enabled, contact your Alvarion representative.

OR

Double click the WEP field value (set to NO by default). The following window is displayed.



**Figure 4-26: Password Dialog Box**

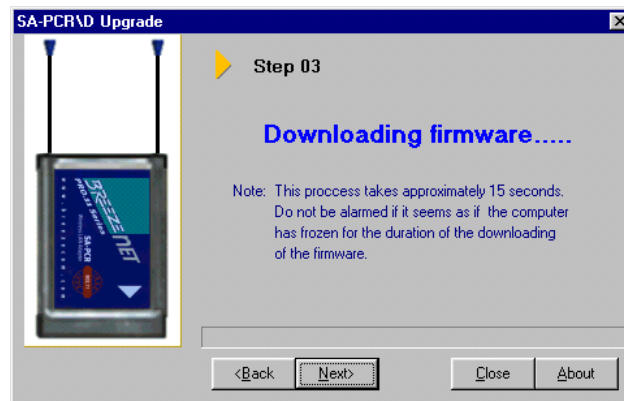
7. Enter the password supplied by Alvarion and click **OK** to return to the Upgrade Program Step 2 window.



**NOTE:**

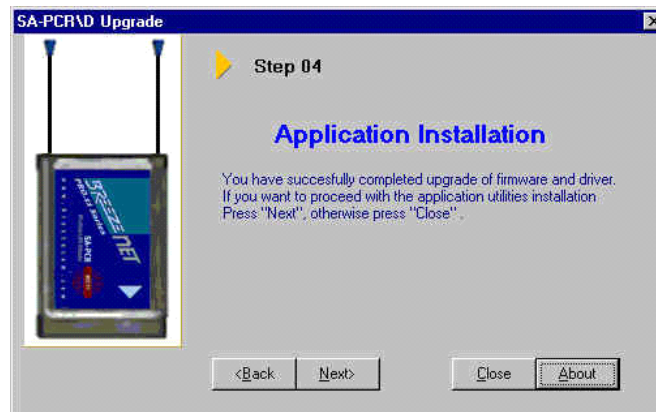
The password for enabling the WEP feature can only be obtained from Alvarion.

8. Follow the on-screen instructions and check the card LEDs.. Click **Next**. The following window is displayed.



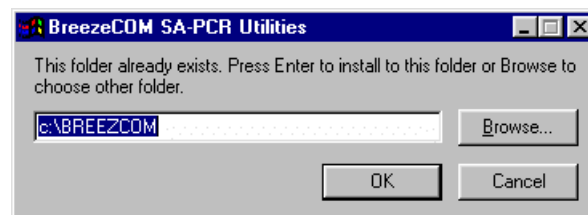
**Figure 4-27: Upgrade Program Step 3**

9. When downloading is complete, the following window is displayed.



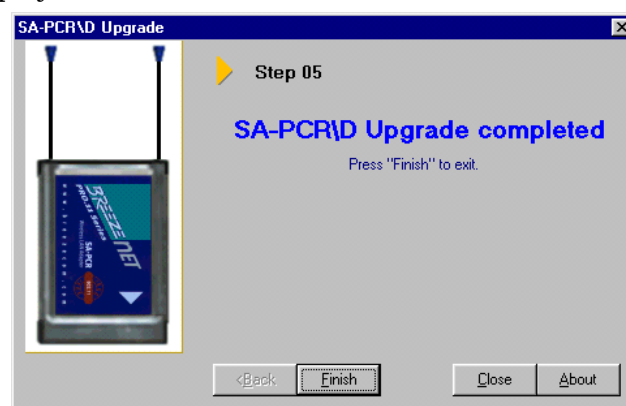
**Figure 4-28: Upgrade Program Step 4**

- 10.** At this point, the Upgrade program installs the SA-PCR utilities.  
Specify the directory to which the program should install the utilities.



**Figure 4-29: Utilities Directory**

- 11.** Continue to follow the on-screen prompts until the following window is displayed.



**Figure 4-30: Upgrade Program Step 5**

- 12.** Restart the computer when prompted. When the computer is restarted the new hardware wizard is entered automatically and the new drivers are installed and shortcuts are updated.

## **Upgrade Procedure for Windows NT, DOS/ODI**

This section describes how to upgrade SA-PCR cards installed in machines running Windows NT or DOS/ODI.

- 1.** Upgrade the firmware in a Windows 95/98 machine using the Upgrade kit program.
- 2.** Remove the old drivers and utilities from your Windows NT or DOS/ODI machine.
- 3.** Download new drivers and utilities from the Alvarion Web site according to your country (<http://www.alvarion.com>).
- 4.** Use the drivers and utilities that you have downloaded to install the new versions of the drivers and utilities.

# Installation Troubleshooting

The following are some problems that may occur while installing the SA-PCR card, and some recommended solutions to these problems. Should you encounter problems during installation that are not listed in this section, contact Alvarion Technical Support.

➤ **Problem 1. Card does not function properly:**

1. Check Device Manager for conflicts with any other devices and drivers.
2. Right click **My Computer, Properties** and then the **Device Manager** tab.
3. Click **Network Adapters** to verify status of BreezeCOM PC card wireless LAN adapter: an exclamation mark next to the card indicates a conflict.

➤ **Problem 2. There is a Resource Conflict, perform the following:**

1. Double click the BreezeCOM Wireless LAN Adapter.
2. Select the *Resources* tab.
3. In the event that the conflicting resources are listed in the conflicting device list, edit the Memory range and Interrupt to values that do not cause conflicts.

➤ **Problem 3. There is no resource conflict, but the card still fails to work. There may be a conflict with DOS drivers not recognized by Windows:**

1. Look for device drivers or lines containing device or call commands in either the autoexec.bat or config.sys files.
2. Disable the conflicting drivers and devices and uninstall and reinstall the card.

# Installing the SA-PCR Drivers in ODI Systems

The ODI driver supports Novell VLM and NETX clients, Novell TCPIP, LANtastic v.6 (with ODINSUP), Microsoft Windows 3.11 (with ODINSUP).

The following files are supplied for the DOS ODI environment:

<b>brzwlan.com</b>	ODI driver file, generic version
<b>brzwlanf.com</b>	ODI driver file for Falcon 310 (supplied only on request)
<b>brzwlan.ini</b>	Default configuration file
<b>brzsetup.exe</b>	Site survey utility
<b>net.cfg</b>	Sample ODI16 configuration file
<b>Brzwlan.ins</b>	Installation information for Novell client (DOS and Windows)

- 1.** The ODI driver gets its resources from the Card & Socket Services. Verify that the PC you are using is installed with Card & Socket Services software.
- 2.** Copy all files from the DOSODI directory on the driver to the NetWare client directory. (In case you already have a NET.CFG file that you want to keep, copy and paste the BRZWLAN section from the sample NET.CFG file, supplied by Alvarion, into your existing file.
- 3.** To login to a NetWare server you should run the following files (make sure that the NET.CFG and the BRZWLAN.INI files are located in the directory from which you run the following files:
  - ♦ LSL.COM (supplied by Novell)
  - ♦ BRZWLAN.COM

- ♦ IPXODI.COM (supplied by Novell)
  - ♦ VLM.EXE (supplied by Novell)
4. After running the BRZWLAN file, the yellow LED on the card should blink several times and then remain lit.

## Configuration Notes

The following lists additional issues that should be considered when performing the configuration.

1. To configure the SA-PCR, use the brzsetup.exe configuration utility.
2. A sample net.cfg file is provided; you may edit this to configure the parameters for IRQ and MEM.
3. For DOS versions 3.30 to 6.20, LASTDRIVE=E by default. If the user only has drive C, letters D and E will be available for Novell network drives. To make all letters available for the network, add LASTDRIVE=Z to the config.sys file.
4. The units can only work with AP-10 PRO. 11 (which have 802.11 software version 4.3 or later).
5. To see the version of the SA-PCR, ensure that the card is inserted and run the Site Survey utility.
6. For configuration of the NDIS2 stack using ODINSUP, refer to the ODINSUP documentation.

## Running the Configuration Utility

This section describes how to run the configuration utility.

1. Change to the NetWare client directory.
2. Type brzsetup and press **Enter**.

3. Enter the ESS ID as defined in the AP (if using default ESS ID, do not change).
4. Reset/restart the computer.

**NOTE:**

Default ESSID is **ESSID1** in capital letters.

## Troubleshooting ODI Installation

The following paragraphs provide information that can help in the event of problems encountered in the ODI drivers installation.

- ◆ It is important to note which net.cfg and brzwlan.ini is used. After installing a new Novell client, two copies of brzwlan.ini, brzwlan.com and net.cfg files may exist, one in the Windows directory and another in the directory where the Novell client is installed.
- ◆ If Card Services fails to provide correct memory and IRQ automatically - edit net.cfg and use IRQ and MEM parameters.
- ◆ If the driver did not display a message `Testing Device`, this indicates that Card Services failed to recognize the card or to provide the required information to the driver. Check the Card Services information configuration.
- ◆ The driver reports an error in allocating IRQ or memory. The Card Services failed to provide the required resources to the driver, or there are no resources available. Reboot without EMM386 or other programs that may take up the adapter memory region. Change the IRQ or MEM parameters in net.cfg to force the driver to request specific resources.
- ◆ The driver reports errors in net.cfg or brzwlan.ini. The files are corrupt or you are not in the correct directory.



- ◆ The yellow LED blinks and turns off after several seconds. The AP is configured with incorrect parameters. Check the AP configuration. The built in antennas are not pulled out or the external antenna is not attached to the PC card.
- ◆ The yellow LED does blink and is not lit. The driver is not receiving interrupts. Try to change IRQ – wrong firmware version or card initialization error.

# Installing the SA-PCR in Linux Systems

The Linux driver supports the following Linux distributions:

- ◆ RedHat 6.0 (kernel 2.2.5-15)
- ◆ Slackware 3.6.0 (kernel 2.0.35)
- ◆ Caldera

Furthermore, the driver is compatible with the following PCMCIA package versions: 3.0.9, 3.0.5, 2.2.7, 2.2.5, and 2.0.36

## ➤ To Check the kernel version:

The command below will give you the version number of the current Linux kernel:

```
# uname -r
```

## Requirements

### ➤ Software

- ◆ Linux system with networking; building environment optional.
- ◆ Installed PCMCIA package.
- ◆ BreezeNET Linux driver (brzcom-x.x.x.tar.gz)

### ➤ Hardware

- ◆ BreezeNET Pro.11 SA-PCR adapter with firmware version 4.4 or higher
- ◆ BreezeNET Pro.11 AP-10 Access Point



**NOTES:**

Firmware version upgrades can be found at: <http://www.alvarion.com>  
The Linux driver does not support firmware updates, therefore updates must be performed from Windows. To check your current firmware version, see *Checking the SA-PCR Firmware Version in Linux*, on page 4-68.

## Installing the PCMCIA Package

Install the package with the distribution's installation tool (e.g. Setup or pkgtool, etc.).

-OR-

Copy the `pcmcia-cs-x.x.x.tar.gz` package (e.g. `pcmcia-cs-3.0.9.tar.gz`) to the Linux kernel source directory (usually `/usr/src/linux`), and unpack it using:

```
gzip -cd pcmcia-cs-x.x.x.tar.gz | tar xfv -.
```

For example:

```
# gzip -cd pcmcia-cs-3.0.9.tar.gz | tar xfv -
```

➤ **To rebuild the PCMCIA binaries (or rebuild the BreezeNET driver):**

1. Change to the kernel source directory and make the configuration (using `make config` or `make menuconfig`):

```
cd /usr/src/linux
```

2. Configure the PCMCIA build environment (using `make config`):

```
cd pcmcia-cs-x.x.x (Where 'x.x.x' represents the PCMCIA card  
services version)
```

3. Make sure that you specify the target directory correctly (usually `/lib/modules/x.x.x`, where 'x.x.x' is the kernel's version).
4. Rebuild the PCMCIA package using `make all` or `make install`.

## Checking the SA-PCR Firmware Version in Linux

This section describes how to establish the version number of the SA-PCR firmware on a system running Linux.

1. Insert the card in a free PCMCIA slot.
2. Change the directory to /usr/src/linux/pcmcia-cs-x.x.x (the directory where you previously unpacked the PCMCIA Card Services):

```
cd to debug-tools and run./dump_cis
```

The output appears as follows:

```
vers_1 4.1, "BreezeCOM", "BreezeNET PC-Card", "Version  
4.4.07 990608"
```

Where "Version x.x.xx" describes the current firmware version of the card.

3. If you previously installed Card Services, perform the following:

```
Run % cardctl ident
```

4. Locate the line using the following command:

```
product info: "BreezeCOM", "BreezeNET PC-Card", "Version  
4.4.07 990608"
```

Where "Version x.x.xx" describes the current firmware version of the card.

## Installing the SA-PCR Linux Driver

This section describes how to install the SA-PCR driver on a system running Linux.

1. Copy the BreezeCOM driver archive to the PCMCIA source directory:

```
cp -fp brzcom-y.y.y.tar.gz /usr/src/linux/pcmcia-cs-x.x.x
(where x.x.x is the PCMCIA card services version and y.y.y is the
breezeCOM driver version).
```

For example:

```
# cp -fp brzcom-0.9.3.tar.gz
/usr/src/linux/pcmcia-cs-3.0.9
```

2. Unpack the driver:

```
gzip -cd brzcom-x.x.x.tar.gz | tar xfv -
```

This creates a 'brzcom' directory, where x.x.x represents the BreezeCOM driver version. For example:

```
# gzip -cd brzcom-0.9.3.tar.gz | tar xfv -
```

3. Copy the driver's binary file to the PCMCIA modules library:

```
cd brzcom
```

```
cp -fp xbrzcom_cs.o /lib/modules/x.x.x/pcmcia (where x.x.x is
the kernel version).
```

For example:

```
# cp -fp xbrzcom_cs.o /lib/modules/2.2.5-15/pcmcia
```

4. Configure the PCMCIA card, the driver and the network as explained in *Configuration Steps Prior to Operation*, on page 4-72.

## Building the Driver

This section describes how to build the driver in Linux.

- 1.** Make sure the kernel build environment and the PCMCIA build environment are set correctly (see *Requirements*, on page 4-66).
- 2.** If you have previously built the driver and want to rebuild it, you may need to clean it using: `make clean`
- 3.** Build the driver using: `make all`
- 4.** Install the driver using: `make install`

**NOTE:**

If your target build directory is NOT the "real" lib/modules directory, you will have to manually copy the file `xbrzcom_cs.o` from the target build to the "real" target.

- 5.** Configure the driver for a different Hopping Standard (Country Domain):
  - ♦ Edit the file `brznet.c` and find the next string:  

```
iprs.cs.countryCode=GetChangedWordFormat(3)
```

- ◆ Change the number to your country code, save it and recompile the driver.

**Table 4-2: Country Domain - Country Code**

Hopping Standard	Number of Sequences per Hopping Set
Australia	20
Canada	10
Europe ETSI	26
France	11
Israel	11
Japan	4
Korea	4
Netherlands	5
Singapore	12
Spain	9
US FCC	26



**NOTE:**

Site Proprietary is not supported in this release.

**IMPORTANT:**

Changing the Country Domain might be against local communication regulations and it is considered illegal if improper setting is configured.

6. Check the driver version of the compiled module:

```
% strings xbrzcom_cs.o |grep version
```

The output looks as follows:

```
Linux Driver version 0.9.3
```

## Configuration Steps Prior to Operation

The following elements must be configured before using the driver:

- ◆ The PCMCIA handler
- ◆ The driver
- ◆ The network
- ◆ Example files

### Configuring the PCMCIA Handler

This section describes how to configuration the PCMCIA handler.

1. Change to the PCMCIA configuration directory:

```
cd /etc/pcmcia
```

2. Using a text editor, open the config file for editing:

```
vi config
```

-OR-

```
pico config (you may need to 'chmod' if the file is set as read-only).
```



3. Look for the section labeled *Device driver definitions*. Under this section you will see several declarations of *device* followed by *class*. Add the following declaration:

```
device "xbrzcom_cs"

class "network" module "xbrzcom_cs"
```

4. Look for the section labeled *Ethernet adapter definitions*. Under this section, you will see several declarations of *card* followed by *version* and *bind*. Add the following declaration:

```
card "BreezeCOM SA PCR-11 Pro"

version "BreezeCOM"

bind "xbrzcom_cs"
```

5. Save and quit.

## Configuring the Driver

This section describes how to configure the driver on a PC running Linux.

1. Change directory to the PCMCIA configuration directory:

```
cd /etc/pcmcia
```

2. Using a text editor, open the options file for editing using:

```
vi config.opts
```

-OR-

```
pico config.opts (you may need to 'chmod' if the file is set as
read-only).
```

3. Add the driver configuration options at the end of the file:

```
module "xbrzcom_cs" opts "ess_id=your_ess_id
irq_list=8,9,10 verbose=0"
```

Where the parameters are defined as the following:

- ♦ **ess\_id** - The ESS ID as defined in the AP. The default ESS ID is ESSID1
- ♦ **irq\_list** - A list of up to 4 IRQ (Interrupt Request) numbers that may be used by the adapter. Consult the adaptor's and your computer's documentation for a list of usable IRQs, or do a 'cat /proc/interrupts' to see which IRQs are already taken. If you are not sure which IRQs to use, remove the irq\_list parameter.
- ♦ **verbose** - Controls diagnostic messages. For full diagnostic messages set to 1 (one). For minimal messages set to 0.

Example: for using the default ESS ID, default IRQs and minimal diagnostic messages:

```
module "xbrzcom_cs" opts "ess_id=ESSID1 irq_list=8,9,10  
verbose=0"
```

## Configuring the Network

This section describes how to configure the network on a PC running Linux.

1. Determine the network address, the Adapter's address and the gateway address. In this section we use the following sample:

Network	169.254.200.0
Gateway	169.254.200.2
Local IP	169.254.200.10 0

2. Configure the network using 'ifconfig' and 'route':

```
ifconfig eth0 169.254.200.100  
  
route add -net 169.254.200.0 eth0
```

```
route add default gw 169.254.200.2
```

3. The file 'brzcfg' contains a script for network configuration; you may edit it, and then run it with: /brzcfg.
4. Edit the 'network.opts' file as follows (you may need to 'chmod' if the file is set as read-only):

```
IPADDR="169.254.200.100"
```

```
NETWORK="169.254.200.0"
```

```
BROADCAST="169.254.200.255"
```

```
GATEWAY="169.254.200.2"
```

```
NETMASK="255.255.255.0"
```



**NOTE:**

To configure the card to work with DHCP, set DHCP=y in network.opts. Make sure that you have installed a DHCP client (such as dhcpcd) on your computer. RedHat 6.0 and above has scripts that handle DHCP automatically (dhcpcd is included in the RedHat release). For other distributions, you may need to adjust the configuration files to autostart the DHCP client upon card insert detection.

Example configurations of the above files can be found in /examples/.  
Make sure to copy these files to /etc/pcmcia directory.

## SA-PCR Operation With Linux

This section describes how to conduct SA-PCR operations on a PC running Linux.

1. Restart the computer.
2. Insert the PCMCIA card. A high-tone beep is heard and the following message is displayed:

```
BreezeNET Pro.11 --- Linux Driver version x.x.x
```

3. After a few seconds, a second high-tone beep is heard, and the initialization message is displayed:

```
BreezeNET Pro.11 ==> Initialized
```

4. If you hear a low-tone beep and the above message does not appear, the configuration was set incorrectly.
5. After initialization, test the connection with Ping or any other communication program.

## Diagnostic Messages

The following diagnostic messages are displayed even if the **verbose** option is set to zero (in `/etc/pcmcia/config.opts`):

```
BreezeNET Pro.11 --- Linux Driver version x.x.x
```

Displayed when the card is inserted.

```
BreezeNET Pro.11 ==> Initialized
```

Displayed after the card is inserted and loaded.

```
BreezeNET Pro.11 ==> Unloaded
```

Displayed after the card is removed.

```
BreezeNET Pro.11 ==> IRQ x Request FAILED
```

Displayed if the IRQ (assigned to the driver by the PCMCIA handler) could not be allocated to the driver.

When this message is displayed the card is inoperable. A different IRQ is needed to be assigned to the card (see Section *Checking the IRQ Status*).

## LED Status

Check the functioning of the AP LEDs.

## Checking the IRQ Status

You can check `/proc/interrupts` for any occurrences of interrupt conflicts:

```
cat /proc/interrupts
```

	CPU0	
0:	216722	XT-PIC timer
9:	155	XT-PIC BreezeCOM Card

If the number of interrupts (in the 2<sup>nd</sup> column) is 0, the card or driver are not working.

## Site Survey

To check the adapter's status and signal levels (Site Survey):

```
cat /proc/net/BreezeCOM
```

The following table is displayed:

```
BreezeCOM SA-PCR WLAN 802.11, Linux driver by Ericsson Radio Systems
```

```
----- Current signal levels for neighbor AP's-----
```

```
Configured ESS-ID: ESSID1
```

-- AP --	---- HW MAC ADDR ----	-- Signal strength --
#0	00:20:d6:81:62:29	*-48 dBm
#1	00:00:00:00:00:00	0 dBm
#2	00:00:00:00:00:00	0 dBm
#3	00:00:00:00:00:00	0 dBm
#4	00:00:00:00:00:00	0 dBm
#5	00:00:00:00:00:00	0 dBm
#6	00:00:00:00:00:00	0 dBm
#7	00:00:00:00:00:00	0 dBm
#8	00:00:00:00:00:00	0 dBm
#9	00:00:00:00:00:00	0 dBm

```
-----
```

\* Indicates the current AP that the SA-PCR card is associated with. The screen is updated automatically every second.

## Chapter 5

# BreezeCONFIG PRO.11 SNMP Configuration Utility



### About This Chapter

The BreezeCONFIG PRO.11 utility is an SNMP-based (Simple Network Management Protocol) application designed to manage PRO.11 system components. The system administrator can use the BreezeCONFIG PRO.11 utility to control a large number of devices from a single location.

- ◆ The BreezeCONFIG PRO.11 utility features:
- ◆ Device status and current configuration verification.
- ◆ Selected device configuration modification.
- ◆ Simultaneous configuration modification of multiple devices.
- ◆ Firmware upgrading for single or multiple devices.
- ◆ Traffic statistic and performance data monitoring.
- ◆ Trap monitoring.

This chapter is comprised of the following sections:

- ◆ **Working with BreezeCONFIG PRO.11**, page 5-2, describes the complete functionality of the BreezeCONFIG SNMP management utility.
- ◆ **Working with Device Configurations**, page 5-37, describes the parameters available in each window of the utility.
- ◆ **Reading Trap Message**, page 5-63, describes how to access trap messages sent from the selected unit to the utility.

## Working with BreezeCONFIG PRO.11

The following sections describe how to work with the featured functionality of the BreezeCONFIG PRO.11 configuration utility.

### Introducing the Configuration Utility Window

The main BreezeCONFIG PRO.11 window, which is referred to as the *Configuration Utility* window, enables you to access a wide array of monitoring and configuration options, which are described in the following sections.

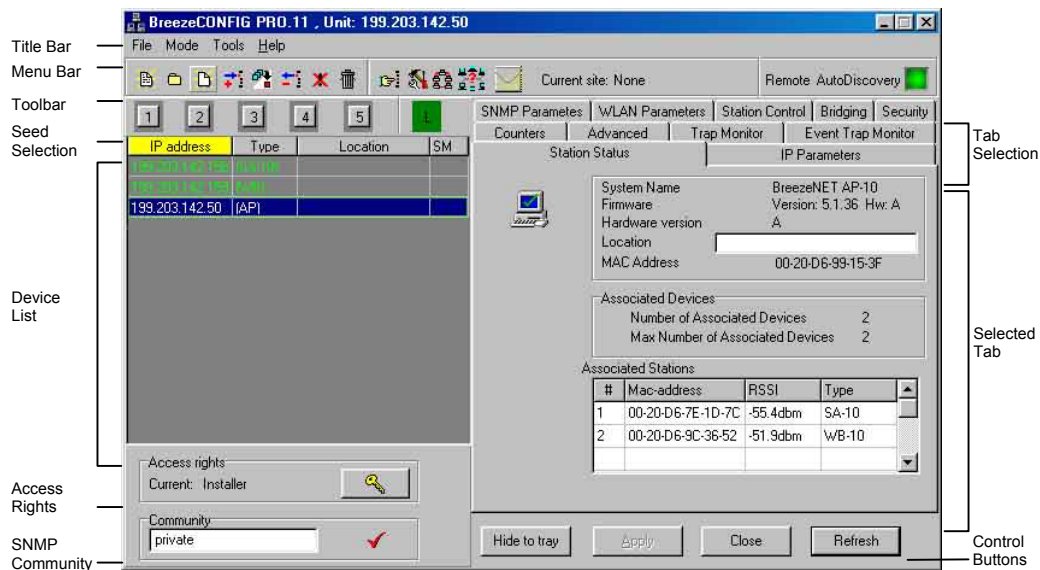
This section describes how to access the *Configuration Utility* window and provides a brief description of each window component.

➤ **To access the Configuration Utility window:**

- 1.** From the Windows *Start* menu, select **Programs** and then select **BreezeCONFIG PRO.11**.



2. From the displayed menu, select **BreezeCONFIG PRO.11**. The *Configuration Utility* window is displayed, as shown below.



**Figure 5-1: Configuration Utility Window**

The *Configuration Utility* window is comprised of the following components:

- ◆ **Title Bar:** Identifies the application and the IP address of the selected device (in Unit Configuration mode) and enables you to minimize, maximize and close the application.
- ◆ **Menu Bar:** Enables you to access multiple options and application functionality. For more information, refer to Working with the Menu Options, on page 5-22.
- ◆ **Toolbar:** The toolbar is comprised of the following buttons.



**Open Site:** Accesses the *Select Site* window and enables you to open a Site file containing a saved list of devices.



**Close Site:** Saves and closes the Site file that is currently open.



**Create New Site:** Enables you to create and open a new Site file.



**Add Device to Site:** Adds the device that is currently selected in the Device List to the Site file that is currently open.



**Add ALL Listed Devices to Site:** Adds all devices currently listed in the Device List to the Site file that is currently open.



**Remove Device from Site:** Deletes the device that is currently selected in the Device List from the Site file that is currently open.



**Remove ALL Listed Devices from Site:** Deletes all devices currently contained in the Device List from the Site file that is currently open.



**Delete Site:** Deletes the Site file that is currently open.



**Locate Unit:** Locates an individual device by its IP address.



**Set IP Address:** Sets a device's IP address based on its MAC address.



**Local Network Autodiscovery:** Automatically discovers stations connected to the local (Ethernet) network.



**Get Seeds Statistics:** Displays the *Device Status* window containing statistics and status indications for all seeds.



**Send Address:** Sends selected addresses to the Firmware Upgrade utility.



**Remote Network Autodiscovery:** Enables you to configure settings for accessing seeds remotely. It also enables you to define the devices that comprise each seed.

For more information, refer to *Working with the Toolbar Options*, on page 5-10.

- ◆ **Seed Selection:** Enables you to select a defined subnet, or seed of devices. In addition, the highest alarm indication for any device in the seed is displayed by color around the selection button. This occurs as long as the Enable/Disable Keep Alive option is selected in the Auto-Discovery Settings window, described in section Remote Network Autodiscovery, on page 5-19.

- ◆ **Device List:** The Device List displays the devices that can currently be managed by the BreezeCONFIG PRO.11 utility.

Each device is displayed according to the device's IP address and device type as well as the device location, which is defined in the *Station Status* tab.


The Device List can be sorted by clicking one of the column headers, for example Type. The list is sorted in ascending order according to the selected column. The default sorting selection is IP Address.

A + sign in the SM column of the Device List indicates the devices included in the Site file that is currently open.

Devices are selected from this list for configuration. To select a device, click the relevant row in the Device List. The entry is highlighted in blue when it is selected. Information is then gathered from the device and displayed in the selected tab area.

In Multiple Configuration mode you can use the standard Windows **Shift** or **Ctrl** key commands to select multiple devices.


- ◆ **Access Rights:** The configuration utility has three access levels, which are designed for different types of users and determine the parameters that can be configured or modified by the user, as follows:
  - ❖ **Technician**, which is the highest level and provides access to all parameters. This level of access rights is reserved for Alvarion technical experts only.
  - ❖ **Installer**, which is the mid-level and provides access to most parameters. This guide is specifically tailored for users with Installer level access rights. Therefore, all parameters described in the guide are accessible to Installer level users.
  - ❖ **User**, which is the lowest level and enables the user only to view parameters. The user level does not permit the modification of any parameters.

To continue modifying the parameters or managing additional devices, you must re-enter the Installer password, by clicking  to display the *Access Rights* window.

The *Access Rights* window also enables you to select a level of access rights and change the Installer password, as shown below:




**Figure 5-2: Access Rights Window**

To set your access rights to Installer or Technician, select the required option in the **New settings** area. Enter the password in the **Password** field and click .

To change the Installer password, enter the required password in the **New Password** field and click .

- ♦ **SNMP Community:** The SNMP Community area enables you to enter a new SNMP community string, which is used by BreezeCONFIG PRO.11 when sending an SNMP request to the selected device(s).

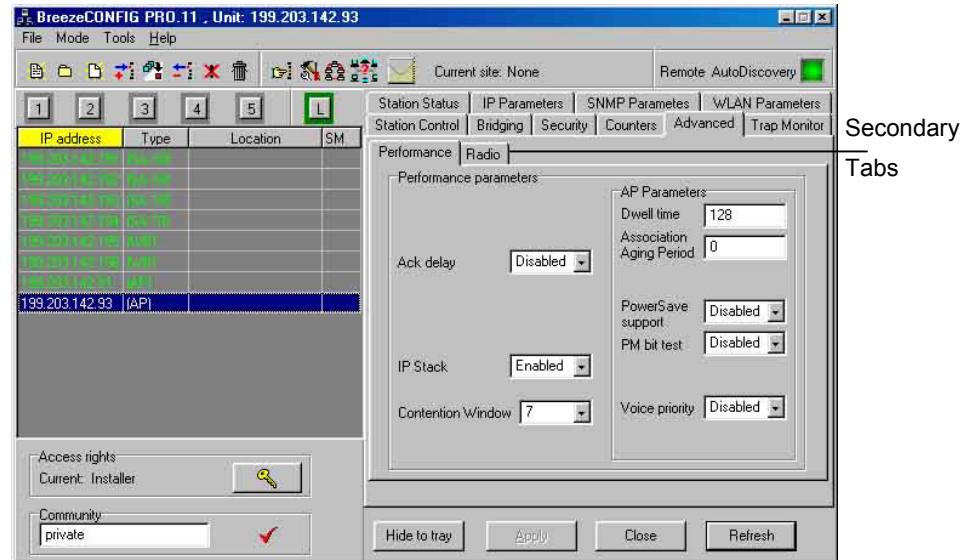
Device information can be viewed only when using its Read or Read/Write community string. Otherwise the device does not appear in the Device List. Configurable parameters can be changed only when using the Read/Write community string.

To change the community string, type the community string in the **Community** field. Then, click  to confirm the new community string.

A device's community string can be modified in the *SNMP Parameters* tab.

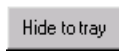
- ◆ **Tab Selection:** The Tab Selection area is comprised of several tabs, each corresponding to a workspace containing a specific group of parameters. The tabs and parameters contained in several of the tabs vary according to device type and SW version. If no device is selected, the Tab Selection area comprises all possible tabs for all device types.
- ◆ **Selected Tab:** The Selected Tab area is a workspace that varies according to the tab selected. The Selected Tab area enables you to view status or performance data and modify specific parameters, depending on the tab selected.


- ◆ **Secondary Tabs:** Certain Selected Tab areas are further divided into multiple workspaces, to provide all required parameters in the selected tab category. In these cases, the Selected Tab area contains a Secondary Tabs area, as indicated below.

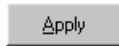


**Figure 5-3: Secondary Tabs**

- ♦ **Control Buttons:** All *Configuration Utility* windows contain the following buttons.



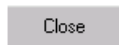
Minimizes the BreezeCONFIG PRO.11 utility. The application is minimized and displayed as  in the system tray. Click the icon to restore the application.



Implements the current modifications.



Updates the information displayed in the window using current values acquired from the device.





Closes the current window without implementing any modifications.

## Working with the Toolbar Options







This section describes how to work with the options available through the BreezeCONFIG ACCESS utility toolbar.

### Working with Site Files

Site files enable you to create, modify and load logical groupings of devices to the Device List. Site files are text files with the extension ste (\*.ste). The toolbar enables you to perform the following operations:

	<p><b>Open Site:</b> Opens an existing Site file. The devices included in the Site file are added to the current list of devices in the Device List. Only one Site file can be open at any time. You can use the Add/Remove functions described below to change the contents of the open Site file.</p>
	<p><b>Close Site:</b> Saves and closes the current Site file. An open Site file must be closed before another Site file is opened.</p>




	<b>Create New Site:</b> Opens a <i>Save As</i> window that enables you to define a name and path for a new Site file. Once the name is defined and saved, the Site file is opened and you can use the Add/Remove functions described below to select the devices to be included in the Site file.
	<b>Add Device to Site:</b> Adds the selected device to the open Site file. A device included in the open Site file is marked with a + sign in the SM column of the Device List.
	<b>Add ALL Listed Devices to Site:</b> Adds all devices currently displayed in the Device List to the open Site file.
	<b>Remove Device from Site:</b> Removes the device that is currently selected in the Device List from the open Site file.
	<b>Remove ALL Listed Devices from Site:</b> Removes all devices currently displayed in the Device List from the open Site file.
	<b>Delete Site:</b> Deletes the Site file that is currently open and sends it to the Recycle Bin.

These functions can also be accessed through the *Tools* menu.

## Locating a Device based on IP Address



The Locate Device feature enables you to find an individual device using its IP address. This includes devices located behind a router, which cannot be detected by the Local Network Autodiscovery mechanism.

➤ **To locate a device using its IP address:**

1. In the toolbar, click , or select **Locate Device** from the *Tools* menu. The *Locate Device* window is displayed, as shown below.



**Figure 5-4: Locate Device Window**


2. In the **Enter IP address** field, enter the IP address of the device to be located and click . Once located, the device information is displayed in the Device List.
3. Click  to close the *Locate Device* window.

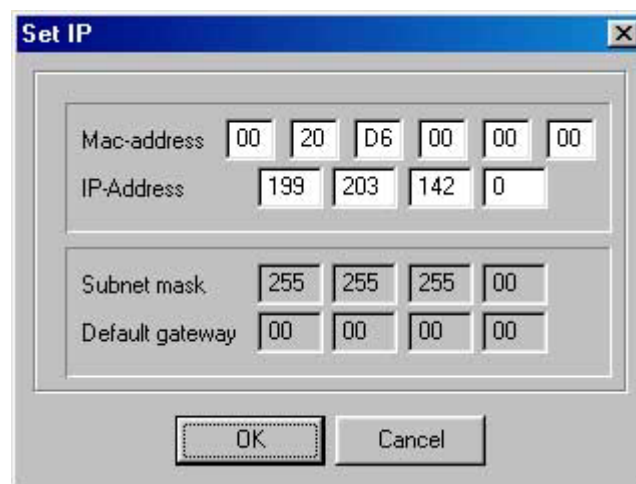
## Setting an IP Address Based on the MAC Address

The Set IP Address feature simplifies the procedure for defining IP address information for newly-added devices that are still defined by their default IP settings. This feature can only be used if the management station is on the same Ethernet segment as the device, and not behind the router.

➤ **To set an IP address:**



1. In the toolbar, click , or select **Set IP** from the *Tools* menu. The *Set IP* window is displayed, as shown below.




Mac-address	00	20	D6	00	00	00
IP-Address	199	203	142	0		
Subnet mask	255	255	255	00		
Default gateway	00	00	00	00		

OK Cancel

**Figure 5-5: Set IP Window**

2. In **Mac-Address** field, enter the device's MAC address.
3. In the **IP-Address** field, enter the required IP address for the device.
4. In the **Subnet mask** field, enter the required subnet mask.
5. In the **Default gateway** field, enter the device's default gateway.


6. Click . The *Set IP* window is closed and a confirmation message is displayed indicating when the modifications are to take effect. In addition, the MAC address is displayed beneath each device IP address.

**NOTE:**

In order to see the device after assigning the IP address, the assigned IP address must be on the same IP subnet as the management station of the BreezeCONFIG PRO.11 utility. Otherwise, use the Locate Device feature, as described on page 5-12, to find the device.

## Local Network Autodiscovery



To initiate the Local Autodiscovery process, in the toolbar, click . The Autodiscovery mechanism detects all stations connected to the local (Ethernet) network. The Device List is updated to reflect the devices/stations identified by the Autodiscovery process.

## Get Seeds Statistics

To view statistics and status indications for all seeds, in the toolbar, click



. The *Device Status* window is displayed, as shown below.


Device Status for 11/06/02 11:19:05				
	Monitored device	NOT Responding device	NOT monitored device	Total number
1st Seed 62.128.34.0	0	0	0	0
2nd Seed	----	----	----	----
3rd Seed	----	----	----	----
4th Seed	----	----	----	----
5th Seed	----	----	----	----
Local	3	0	0	3
OK				

**Figure 5-6: Device Status Window**

The status/alarm indicators are displayed, as follows:

- ◆ **Green:** Illuminated if the devices responded normally to the most recent query.
- ◆ **Yellow:** Illuminated if one or more devices did not respond to one query.
- ◆ **Red:** Illuminated if one or more devices did not respond to two consecutive queries.

Since the display is static and not updated in real-time, you must close the window and reopen it to view updated information.

Click  to close the *Device Status* window.

## **Sending Addresses to the Firmware Upgrade Utility**


In Unit Configuration mode, the Send Address feature enables you to forward device information from the main BreezeCONFIG Device List to the Device List of the Firmware Upgrade utility.

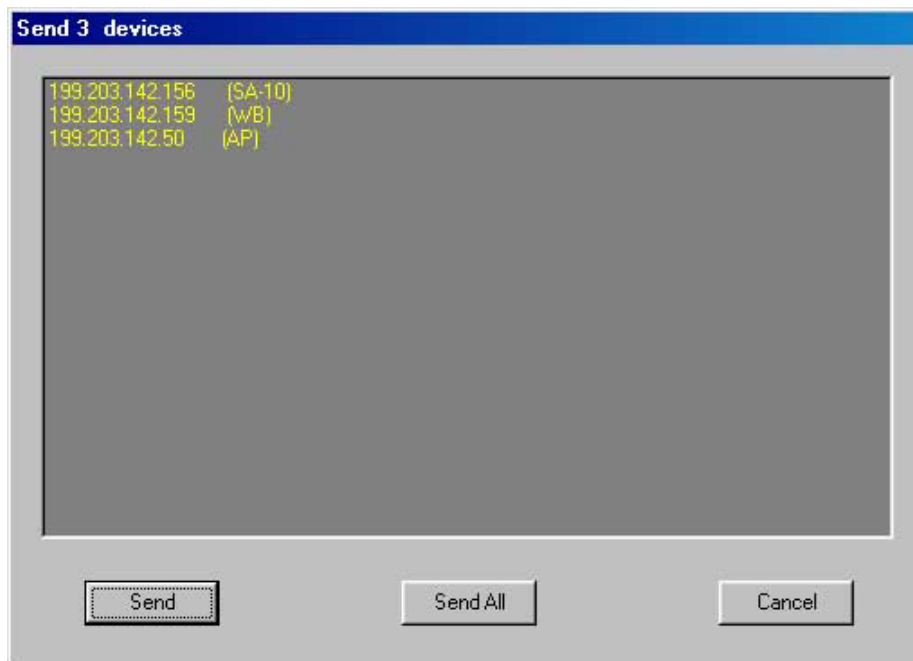


### **NOTE:**

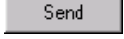

For the Send Address feature to function, the *Firmware Upgrade* window must be open. For more information on working with the *Firmware Upgrade* window, refer to *Working with the Firmware Upgrade Utility*, on page 5-32.

➤ **To send addresses to the Firmware Upgrade utility:**

1. In the toolbar, click . The *Send # Devices* window is displayed, as shown below. Each entry in the list includes the device IP address and device type. The list is sorted by device type.




**Figure 5-7: Send Devices Window**

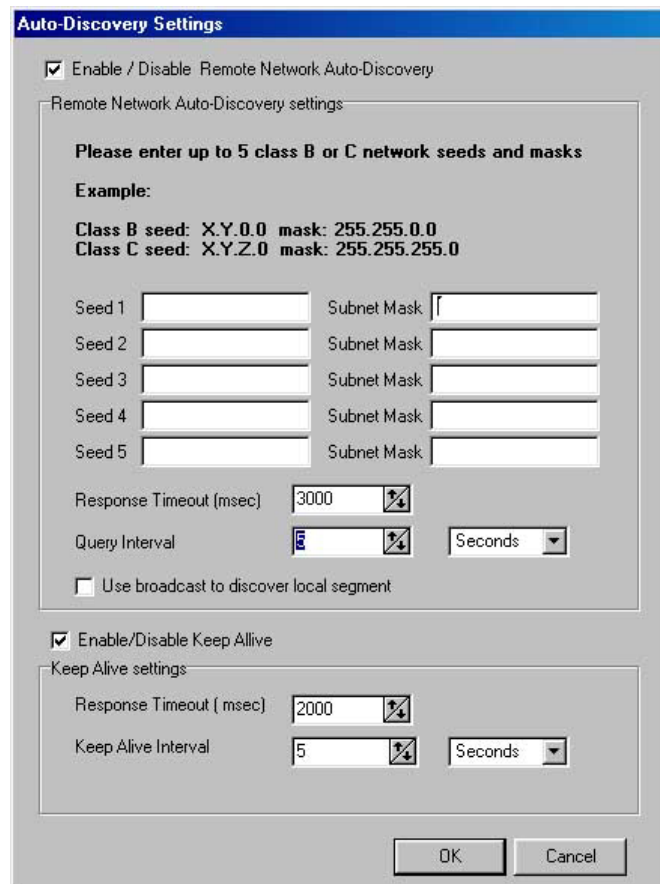
2. To select a device, click to highlight the relevant row in the Send Devices window. You can use the **Shift** and **Ctrl** keys to select multiple devices.
3. Click  to send the selected devices to the Device List of the Firmware Upgrade utility,  
Or  
Click  to send all devices displayed in the list to the Device List of the Firmware Upgrade utility.



## Remote Network Autodiscovery

The *Auto-Discovery Settings* window enables you to configure the settings that enable accessing and monitoring devices located behind routers. In addition, you can configure the make-up of the remote subnets.

To access the *Auto-Discovery Settings* window, click . The *Auto-Discovery Settings* window is displayed.



**Auto-Discovery Settings**

☒ Enable / Disable Remote Network Auto-Discovery

Remote Network Auto-Discovery settings

Please enter up to 5 class B or C network seeds and masks

Example:  
Class B seed: X.Y.0.0 mask: 255.255.0.0  
Class C seed: X.Y.Z.0 mask: 255.255.255.0

Seed	Subnet Mask
Seed 1	
Seed 2	
Seed 3	
Seed 4	
Seed 5	

Response Timeout (msec): 3000

Query Interval: 5 Seconds

☐ Use broadcast to discover local segment

☒ Enable/Disable Keep Alive

Keep Alive settings

Response Timeout (msec): 2000

Keep Alive Interval: 5 Seconds

OK Cancel

**Figure 5-8: Auto-Discovery Settings Window**

The *Auto-Discovery Settings* window is comprised of the following components:

◆ **Remote Autodiscovery Settings**

- ❖ **Enable/Disable Remote Network Auto-Discovery:** Enables you to activate the remote auto-discovery mechanism.
- ❖ **Seed 1 to 5:** Enables you to define up to five Class B or Class C subnet seeds.
- ❖ **Subnet Mask:** For each seed, enter the subnet mask that enables the BreezeCONFIG PRO.11 utility to identify the devices that comprise the associated subnet.
- ❖ **Response Timeout (msec):** Click the up and down arrows to define, in milliseconds, the amount of time that the application waits to receive a response from each address included in the subnet before deciding that the IP address does not exist.
- ❖ **Query Interval:** Click the up and down arrows to define the amount of time that the application waits before querying the next IP address. This prevents overloading the system with queries.
- ❖ **Time Units:** In the related field, next to the **Query Interval** field, select the time device for the value configured in the **Query Interval** field. You can select **Seconds**, **Minutes** or **Hours**.
- ❖ **Use broadcast to discover local segment:** Selecting this option enables the application to query all local devices as well as remote. This saves time in the querying process if a seed is in the local segment.

◆ **Keep Alive Settings**

- ❖ **Enable/Disable Keep Alive:** If enabled, the application continues to query the devices constantly for monitoring purposes. This enables the application to periodically update the *Device Status* window and the seed indicators in the Seed Selection bar.

- ❖ **Response Timeout (msec):** Click the up and down arrows to define the amount of time, in milliseconds, that the application waits for a response to a keep alive query before updating the alarm indication.
- ❖ **Keep Alive Interval:** Click the up and down arrows to define the amount of time that the application waits before the next keep alive query. This prevents overloading the system with keep alive queries.
- ❖ **Time Units:** In the related field, next to the **Keep Alive Interval** field, select the time device for the value configured in the **Keep Alive Interval** field. You can select **Seconds**, **Minutes** or **Hours**.

## Seed Selection

The Seed Selection area enables you to select any of the 5 seeds, which are numbered 1 through 5. You can also select the local network, which is marked with the letter L. Selecting any of the seeds or the local network in the Seed Selection area displays the devices contained in the seed or local network in the Device List.

The background color of each button indicates the current status of the subnet, as follows:

- ◆ **Green:** All devices responded normally to the most recent query.
- ◆ **Yellow:** At least one device did not respond to the most recent query.
- ◆ **Red:** At least one device did not respond to two or more of the most recent queries.

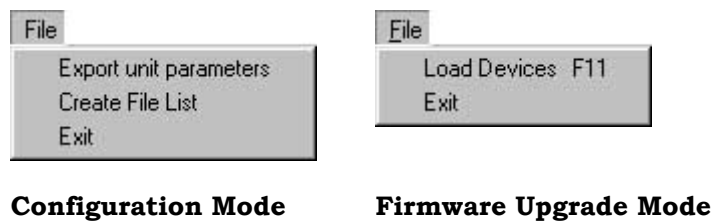
## Working with the Menu Options

The following sections describe the various options available through the BreezeCONFIG PRO.11 menu bar. Note that the menus differ depending on the selected mode.

### File Menu

The *File* menu available in the configuration mode is different than the menu available in firmware upgrade mode, as shown below.

The *File* menu enables you to access various operations that support the featured functionality of the BreezeCONFIG PRO.11 utility, as shown below.



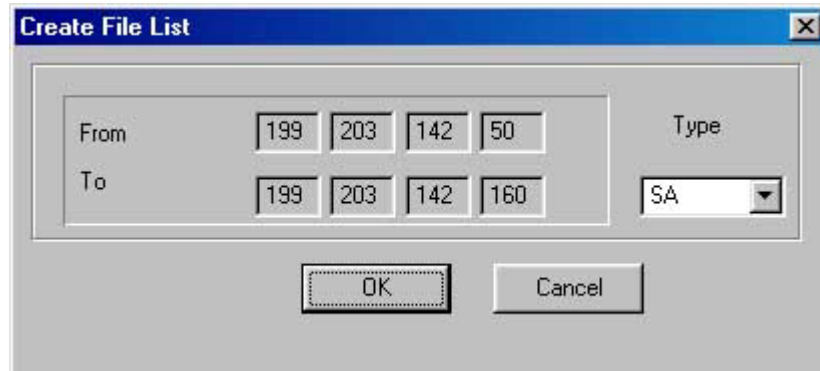
**Figure 5-9: File Menus**

The *File* menu is comprised of the following options:

- ♦ **Export device Parameters:** In Unit Configuration mode, this option enables you to save the configuration of a selected device to a file. By selecting **Export Unit Configuration** from the *File* menu or by clicking the **Export** button in the *Station Control* tab, the *Save As* window is displayed. Enter a file name and select a directory to save the configuration file as a BreezeNET configuration file, with the extension.Brz. The BreezeNET configuration file includes the configuration, status and counters of the selected device.

- ◆ **Create File List:** This option enables you to create a Site file based on a range of IP addresses, as follows:

1. From the *File* menu, select **Create File List**. The *Create File List* window is displayed, as shown below.



**Figure 5-10: Create File List Window**

2. In the **From** field, enter the first IP address to be included in the range.
3. In the **To** field, enter the last IP address in the range.



**NOTE:**

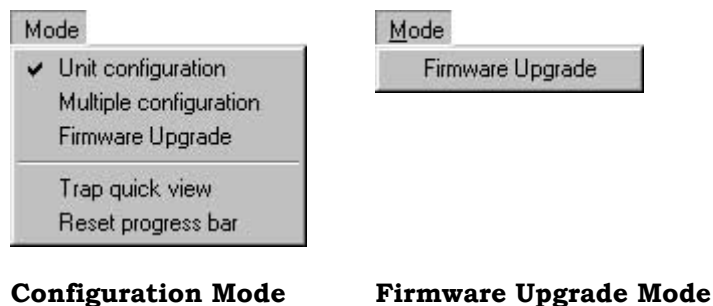
It is recommended that only IP addresses of existing devices be included in the defined range. When the list is loaded, the application searches for each device included in the list. If non-existent addresses are included, this prolongs the searching process. Therefore, it is recommended that, if necessary, two or several lists be created to limit the number of invalid IP addresses for which the application must search.

4. In the **Type** field, from the dropdown list, select the type of device to be included in the device Site file.
5. Click **OK**. The **Save As** window is displayed, where you can enter a file name and select a directory to save the Site file. The file is saved as an.ste file.

- ◆ **Load Devices:** The option enables you to load a list of devices that are saved as a Site file to the *Firmware Upgrade* window. The *Select Site* window is displayed, enabling you to select the required Site file, which is saved with the extension.ste.
- ◆ **Exit:** This option closes the BreezeCONFIG PRO.11 utility.

## Mode Menu

There are several modes in which you can operate the BreezeCONFIG PRO.11 utility. These modes are selected through the *Mode* menu, which is shown below. The selected option(s) is indicated by a dot or checkmark. The Mode menu differs between the configuration and firmware upgrade modes, as shown below.



**Figure 5-11: Mode Menus**

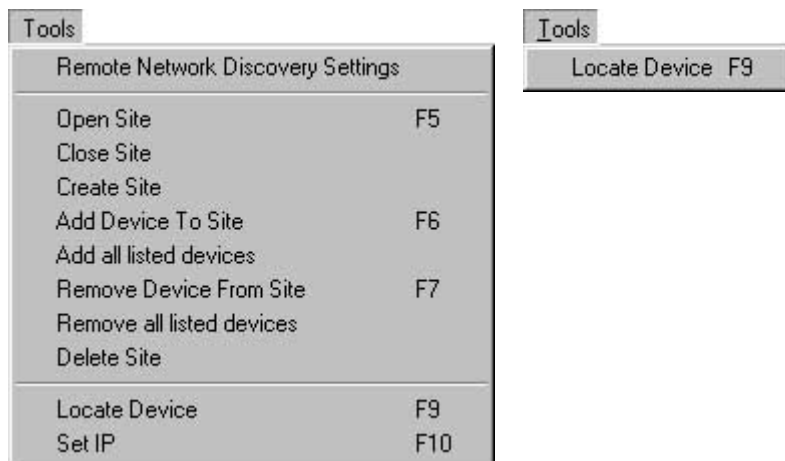
The *Mode* menu is comprised of the following options:

- ◆ **Unit configuration:** This is the default mode, which is used for viewing and/or setting the parameters of a single selected device. For more information, refer to *Working in Unit Configuration Mode*, on page 5-27.
- ◆ **Multiple configuration:** This mode is used for preparing and downloading configuration parameters to multiple devices simultaneously. For more information, refer to *Working in Multiple Configuration Mode*, on page 5-28.

- ◆ **Firmware Upgrade:** Select this mode to launch the Firmware Upgrade utility, which enables you to upgrade the embedded software in multiple managed devices. For more information, refer to *Working with the Firmware Upgrade Utility*, on page 5-32.
- ◆ **Trap quick view:** When set to this mode, the management station switches automatically to the Trap Monitor tab, if a trap message is received and if the management station is included in the list of trap host stations for the selected device. The trap host stations for a selected device can be defined in the SNMP Parameters tab. In addition, to view the traps, the trap sending option in the SNMP Parameters tab for the selected device must be enabled. This option is only operational in Unit Configuration mode. The default is deselected, which means not active.
- ◆ **Reset progress bar:** Displays a progress bar each time a device is reset. This may slow the application since no other operations may be performed simultaneously.

## Tools Menu

The *Tools* menu, which differs in the configuration and firmware upgrade modes, provides access to device definition and location functions that are also available through the toolbar, as shown below.



### Configuration Mode

### Firmware Upgrade Mode

**Figure 5-12: Tools Menus**

The *Tools* menu is comprised of the following options:

- ◆ **Remote Network Discovery Settings:** Enables you to configure settings for accessing devices located behind a router and define the devices that comprise each remote subnet. For more details refer to *Remote Network Autodiscovery* on page 5-19.
- ◆ **Site file operations:** (Open Site, Close Site, Create Site, Add Device To Site, Add all listed devices, Remove Device From Site, Remove all listed devices, Delete Site) The functionality is the same as the corresponding buttons in the Toolbar. For more details refer to *Working with Site Files* on page 5-10.



- ◆ **Locate Device:** This option enables you to find an individual device using its IP address. This includes devices located behind a router. For more information, refer to *Locating a Device Based on IP Address*, on page 5-10.
- ◆ **Set IP:** This option enables you to set the IP address for a device based on its MAC address. For more information, refer to *Setting an IP Address Based on the MAC Address*, on page 5-13.

## Help Menu

Selecting **About** from the *Help* menu enables you to view version and product information regarding the current BreezeCONFIG PRO.11 application. In addition, the *About* window provides a link to the Alvarion website.

## Working in Unit Configuration Mode

The Unit Configuration mode enables you to view the current configuration of a selected device and modify the values of all relevant device parameters. For a description of each configurable parameter, refer to *Chapter 3, Working with Device Configurations*.

The Device List on the left side of the main *Configuration Utility* window can be loaded with updated device information using any one of the following mechanisms:

- ◆ **Select Subnet:** Select one of up to 6 subnets from the Seed Selection area. This includes seeds 1 through 5 and the local network, which is marked with the letter L.
- ◆ **Locate Device:** For a description of how to work with this feature, refer to *Locating a Device based on IP Address*, on page 5-10.
- ◆ **Load Devices:** For a description of how to work with this feature, refer to *File Menu*, on page 5-22.

- ◆ **Open Site:** For a description of how to open a Site file, refer to *Working with Site Files*, on page 5-10.

Each time you select a new subnet or implement the Local Network Autodiscovery feature, if the selected subnet is the local network, the Device List is reset. Therefore, it is recommended that you start by selecting the required subnet and activating the Local Network Autodiscovery feature, if required. Then, you can add additional devices using the Locate Device, Open Site and Load Devices features.

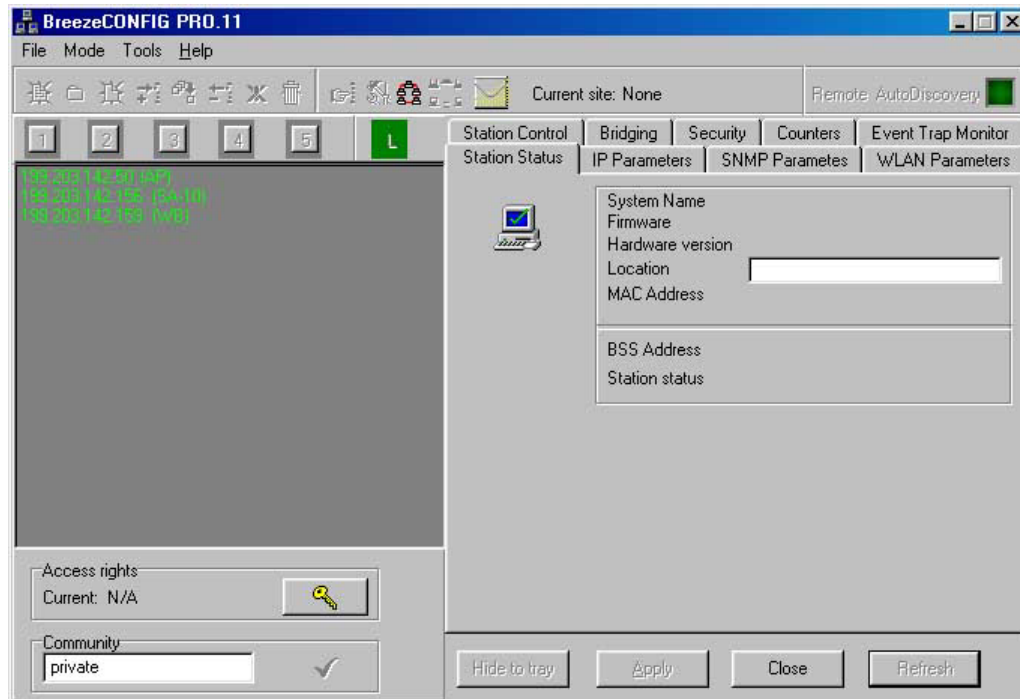
To select a device to review or update its configuration, click the relevant row in the Device List. When selected, the entry is highlighted in blue. Information is then gathered from the device and displayed in the selected tab area.

## Working in Multiple Configuration Mode

The Multiple Configuration mode enables you to download configuration parameters to multiple devices simultaneously, including various device types, such as Access Points, Station Adapters and Workgroup Bridges.

When this option is selected in the *Mode* menu, all relevant configuration fields become write-only, while the irrelevant fields are disabled. In single Unit Configuration mode, some tabs may include only those parameters that are applicable to the specific device selected. For example, parameters that are specific to Access Points are not displayed if the selected device is a Station Adapter.

In Multiple Configuration mode, all the tabs, except the *Advanced* tabs are available, including those that are only available for specific device types in Unit Configuration mode. Each configuration tab includes all relevant parameters, including those that are only applicable to specific device types.



**Figure 5-13: Multiple Configuration Mode**




**NOTE:**

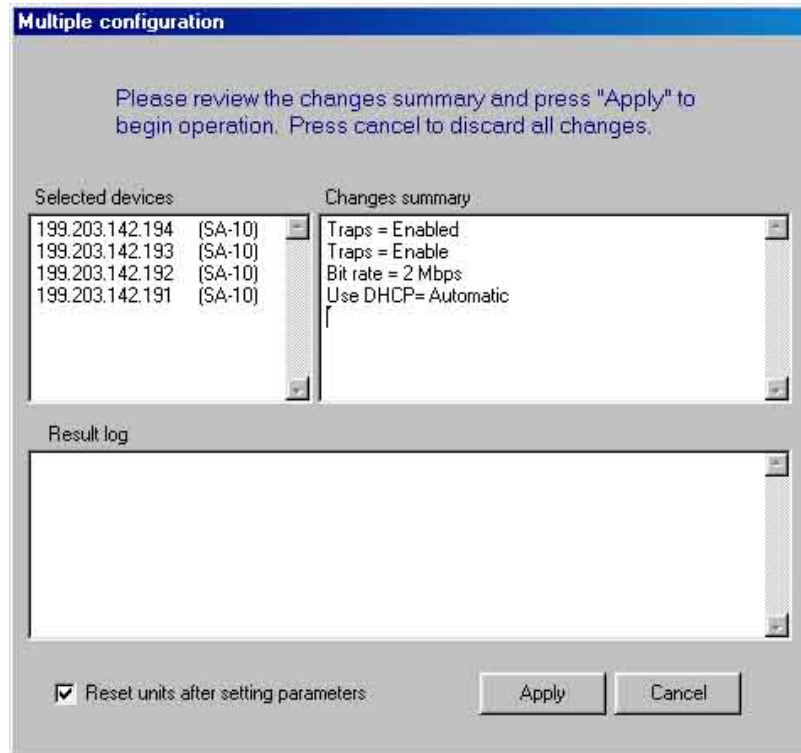
If a parameter is configured that is not applicable to a certain device type, the device is not successfully configured. For example, if the **Bridging Mode** parameter is configured and uploaded to SA or WB devices, where this parameter is not supported, then the configuration for all of these devices fails.

When the Multiple Configuration mode is selected, the devices currently listed in the Device List of the Unit Configuration mode are automatically uploaded to the Device List in Multiple Configuration mode. The Local Network Autodiscovery feature can be used to update the Device List with devices in the local network, if required.

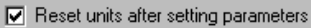
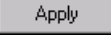
➤ **To modify multiple Unit Configurations:**

1. From the Device List of the main *Configuration Utility* window, select the devices requiring configuration modification. Use the standard Windows **Shift** or **Ctrl** key commands to select multiple devices.

2. In the relevant configuration tabs, modify the required parameters and click . For a description of each configurable parameter, refer to *Chapter 3, Working with Device Configurations*. The *Multiple Configuration* window is displayed, as shown below.



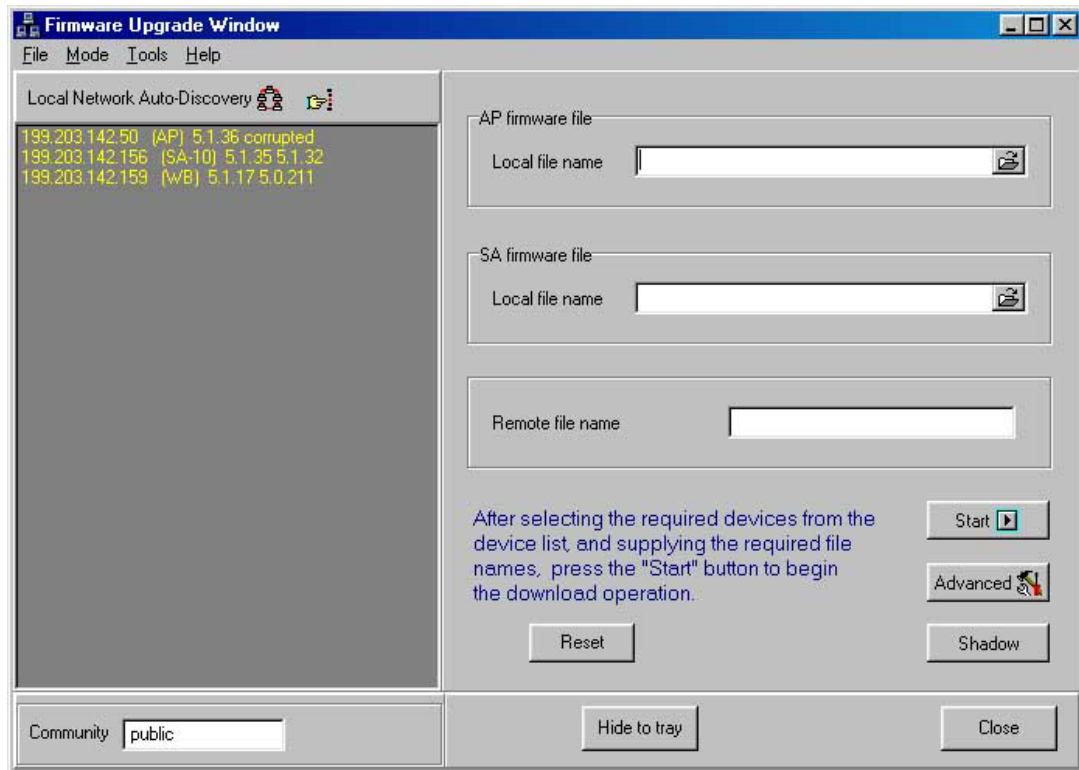
**Figure 5-14: Multiple Configuration Window**

3. The *Multiple Configuration* window displays the selected devices and a list of the configuration modifications made during the current multiple configuration session. Check the  box to reset all affected devices after loading the configuration modification. Click  to load the configuration modification to the selected devices. A log of the multiple configuration session is displayed during and after the operation.

## **Working with the Firmware Upgrade Utility**

The Firmware Upgrade utility enables you to upgrade the embedded device software and determine the current active software version for multiple managed devices. New software versions can be simultaneously downloaded to multiple devices of any type, such as Access Points (AP), Workgroup Bridges (WB), or Station Adapters (SA).

To access the Firmware Upgrade utility, from the *Mode* menu, select **Firmware Upgrade**. The *Firmware Upgrade Window* is displayed, as shown below.





**Figure 5-15: Firmware Upgrade Window**

The Device List is displayed in the left side of the window. Each entry includes the device IP address, device type, current software version and the shadow software version.

When the Firmware Upgrade utility is accessed, the current Device List in the main *Configuration Utility* window is automatically loaded to the Device List of the Firmware Upgrade utility. Once the Firmware Upgrade utility is opened, the Send Address feature in the *Configuration Utility* window can be used to send a list of devices to the Firmware Upgrade utility. The Local Network Autodiscovery feature can be used to update the information for devices in the local network. The Device List can also be loaded with device information using the **Load Devices** option in the *File* menu. Once the **Load Devices** option is selected, the current list is deleted and replaced. The Device List can also be updated by adding devices using the Locate Devices feature.

➤ **To upgrade device software:**

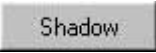

1. Select the devices to be upgraded from the Device List on the left side the window. Use the standard *Windows* **Shift** and **Ctrl** key commands to select multiple devices.
2. You can define the path to the required upgrade file in the applicable **Local file name** fields, or click the button on the right side of each of the selection fields to open the *Select firmware filename* window. There are separate selection fields for Access Points and Station Adapters/Workgroup Bridges.
3. In the **Remote file name** field, enter the applicable remote filename password for the file to be loaded. The password is <read/write community string>.<file extension>. The default read/write community string is **private**.
4. Click  to initiate the firmware upgrade. A log of the upgrade process is displayed after the operation.
5. Click  to modify the settings of the TFTP session used in the upgrade download, as follows:



- ◆ **Packet Timeout (Sec):** Defines the time, in seconds, for which the upgrade process waits for an acknowledgement message. The range is **1** to **30** seconds and the default is **3** seconds.
- ◆ **Packet Retries:** Defines the maximum number of retries, which is the number of times a packet is retransmitted when an acknowledgement is not received within the defined timeout period. The range is **1** to **5** and the default is **3** retries.
- ◆ **Session Retries:** Defines the number of times the TFTP session is retried before determining that the upgrade procedure has failed. The range is **1** to **5** and the default is **3** retries.
- ◆ **Number of Parallel Sessions:** Defines the maximum number of TFTP sessions that can be conducted simultaneously. The range is **1** to **10** and the default is **10**. In the event of too many failures in the upgrade process it is advised that you reduce the value of this parameter.
- ◆ **Save to External Log:** Defines whether the results of the upgrade process are saved to a Log File. The default is **Yes**.
- ◆ **Log File Name:** Enables you to define the name and path to the external Log File. Click the icon on the right to open a *Save As* window, which enables you to navigate to the required location and/or file.
- ◆ **Conditional Downloading:** When defined as **Different**, the download operation occurs only if the version number, as defined in the following parameter, is different from the number of the current version in the device. When configured to **Always**, the version is always downloaded without checking the version numbers. The default is **Always**.
- ◆ **Version Number:** When the **Conditional Downloading** parameter is defined as **Different**, this field is used to define the version number of the downloaded firmware.

➤ **To work with the active and shadow software versions:**

The active firmware version of multiple devices can be managed as follows:

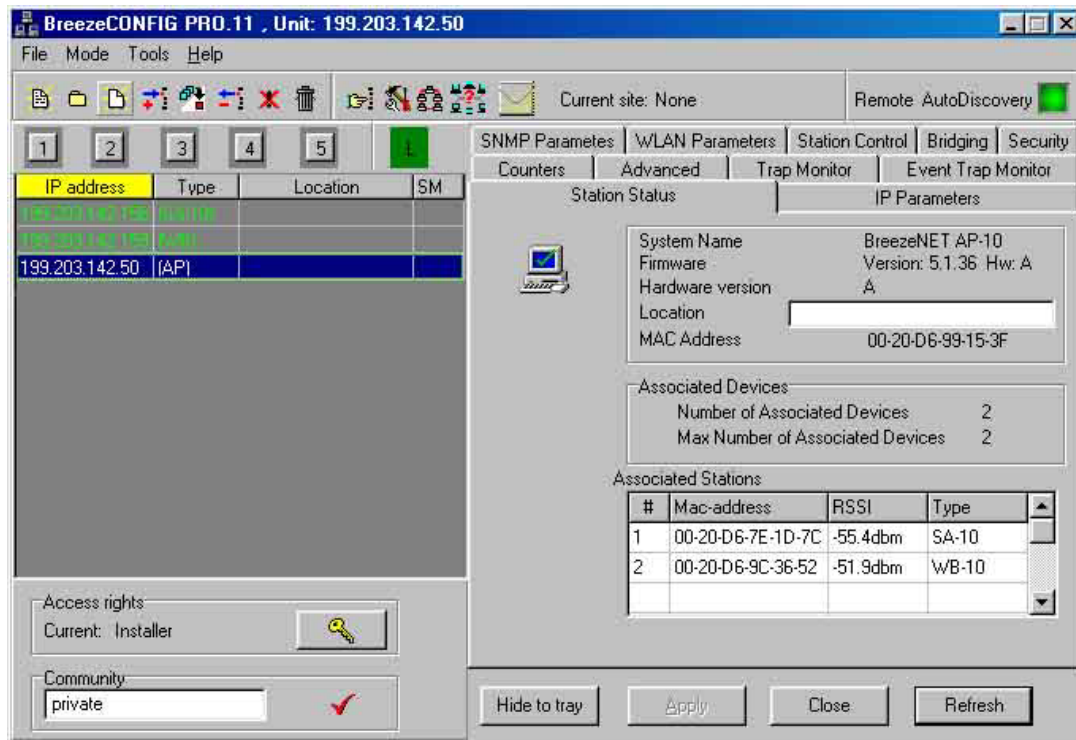
- ◆ Click  to use the Shadow software version in the selected devices after the next reset. The Shadow software is the version that is not currently active.
- ◆ Click  to reset the selected units following the download procedure.

# Working with Device Configurations

Many of the configuration parameters provided by BreezeCONFIG PRO.11 are dependent on the type of device that is being configured and its frequency band. This means that there are different windows and parameters depending on whether an Access Point (AP) or Workgroup Bridge/Station Adapter (SA/WB) is being configured. Note that Station Adapters (SA) have the same configurable parameters as Workgroup Bridges. Therefore, all parameters described for Workgroup Bridges apply to both types of device. For detailed information on each of the parameters refer to the *User's Guide*.

## Station Status

The *Station Status* tab enables you to define the location of the selected device and provides information regarding the current functioning of the device. The *Station Status* tab for APs differs from the *Station Status* tab for WBs and SAs, which is clearly indicated in the description of the tab components.



**Figure 5-16: Station Status Tab – Access Point**

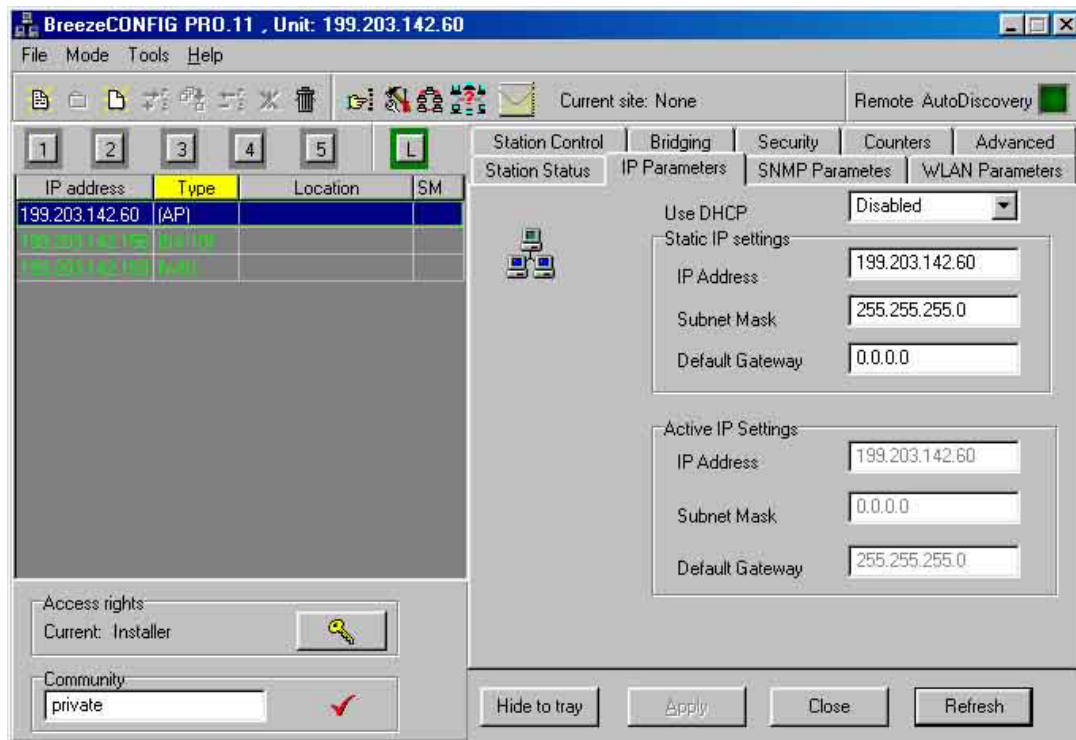
The *Station Status* tab is comprised of the following components:

- ◆ **System Name:** Displays the device type, which identifies the device's function.

- ◆ **Firmware:** Displays the device's current software and hardware version.
- ◆ **Hardware version:** Displays the device's hardware version.
- ◆ **Location:** Displays the location of the selected device. To change the location, in the text box, enter a new location for the device.
- ◆ **MAC Address:** Displays the selected device's MAC address.
- ◆ **Number of Associated Devices (AP only):** Displays the number of devices that were associated with the selected Access Point since the last reset.
- ◆ **Max Number of Associated Devices (AP only):** Displays the maximum number of devices that can be associated with the Access Point at any given time.
- ◆ **BSS Address (WB, SA only):** Displays the BSS address of the Access Point with which the device is currently associated.
- ◆ **Station status: (WB, SA only):** Displays the current association status of the device. The possible statuses are Scanning and Associated.
- ◆ **Associated Stations (AP only):** Displays the list of devices that are currently associated with the selected AP. The information includes the MAC address of the associated device, the average level at which the AP receives signals from the relevant device and the device type.
- ◆ **Neighboring APs (WB, SA only):** Displays additional APs in the vicinity of the selected WB or SA device with which it can associate. The display includes the MAC address of the AP device and the link quality.

## IP Parameters

The *IP Parameters* tab enables you to define IP parameters for the selected device and determine its method of IP parameter acquisition. The IP Parameters tab is identical for all devices.



**Figure 5-17: IP Parameters Tab**

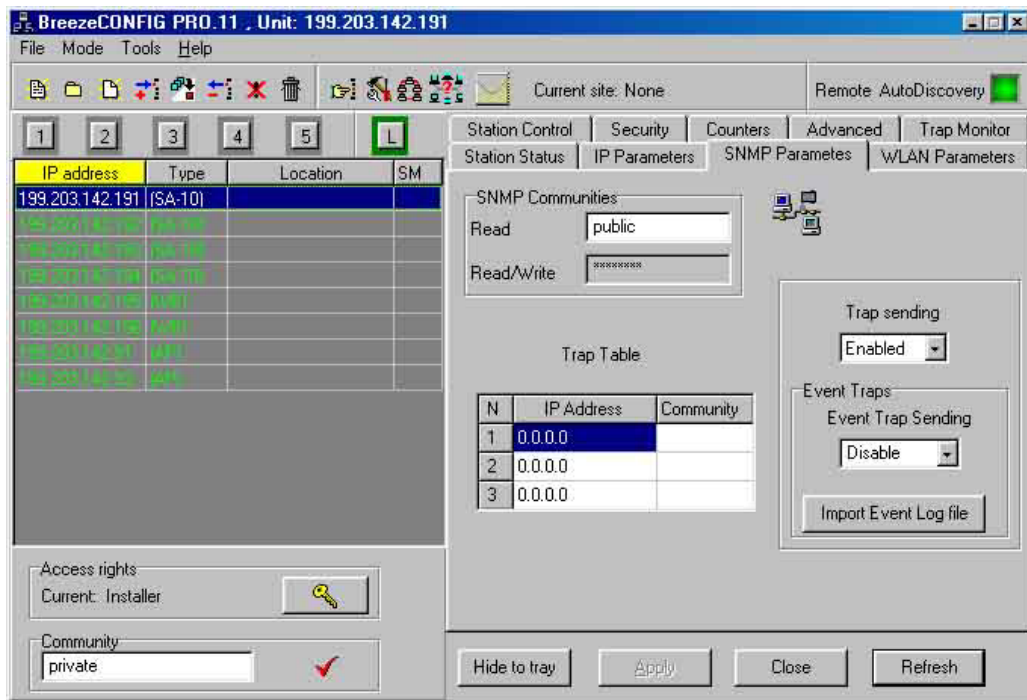
The *IP Parameters* tab is comprised of the following components:

- ◆ **Use DHCP:** From the dropdown list, select an operational mode for the DHCP mechanism, from the following options:
  - ❖ Select **Disabled** to configure the IP parameters manually. The device then operates using the defined static IP parameters.
  - ❖ Select **DHCP Only** to cause the device to search for and acquire its IP parameters, including the IP address, subnet mask and default gateway, from a DHCP server. If this option is selected, configuring the static IP parameters is not required.
  - ❖ Select **Automatic** to cause the device to search for a DHCP server and acquire its IP parameters from the server. If a DHCP server is not located within approximately 40 seconds, the currently configured static parameters are used.  
The default selection is **Disabled**.
- ◆ **Static IP Settings**
  - ❖ **IP Address:** Enter a static IP address for the selected device.
  - ❖ **Subnet Mask:** Enter a static subnet mask for the selected device.
  - ❖ **Default Gateway:** Enter an address for the device's default gateway.
- ◆ **Active IP Settings**
  - ❖ **IP Address:** Displays the device's current IP address.
  - ❖ **Subnet Mask:** Displays the device's current subnet mask.
  - ❖ **Default Gateway:** Displays the device's current default gateway.

## SNMP Parameters

The *SNMP Parameters* tab enables you to define the SNMP Community read and read/write passwords and configure settings related to trap messages and log files.

The *SNMP Parameters* tab is identical for all devices.



**Figure 5-18: SNMP Parameters Tab**

- ◆ **SNMP Communities**
  - ❖ **Read:** Enter the read-only community string, which serves also as the read-only password.
  - ❖ **Read/Write:** Enter the read/write community string, which serves also as the Installer password.
- ◆ **Trap sending:** From the dropdown list, select whether sending traps messages from the device is to be **Enabled** or **Disabled**.
- ◆ **Event Trap Sending:** From the dropdown list, select whether sending traps messages from the device is to be **Enabled** or **Disabled**.

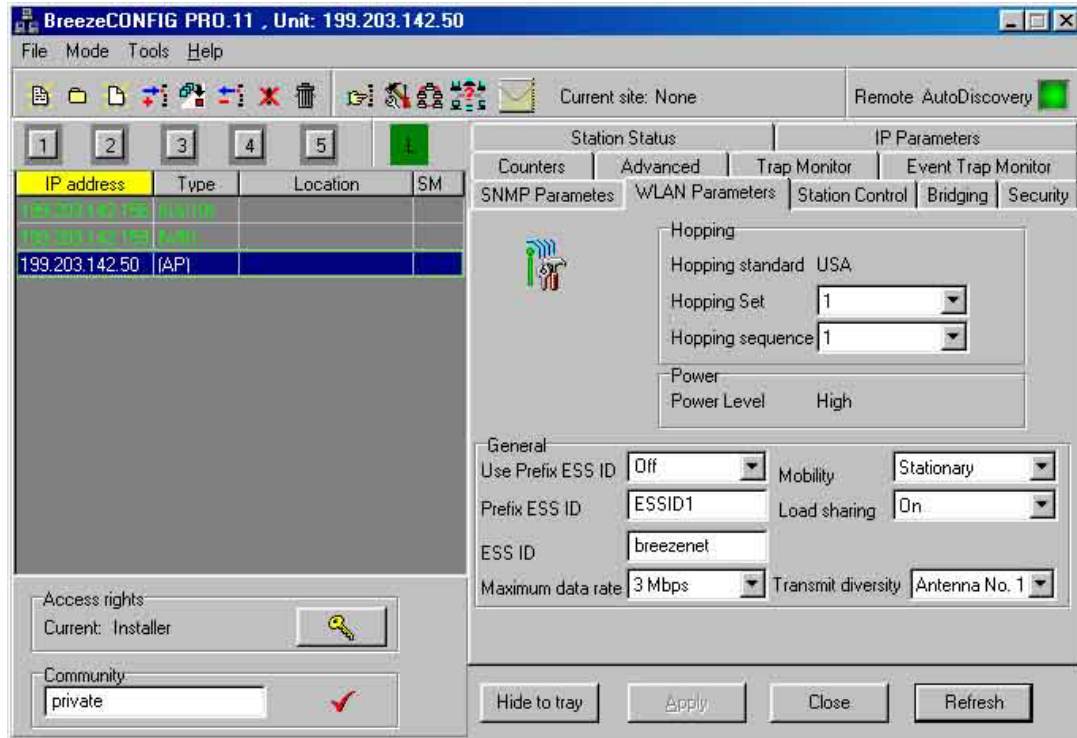


- ◆ **Import Event Log File:** Click to open a Save As window, enabling you to define a name and location for the event log import file.
- ◆ **Trap Table:** To define a station that is to receive trap messages from the selected device, select a row in the IP Address column and enter the station's IP address. Then, select the adjoining field in the Community column and enter the required community string.

## WLAN Parameters

The *WLAN Parameters* tab enables you to configure hopping settings for the selected devices. In addition, you can define ESSID, load sharing, data rate, mobility and antenna diversity parameters.

The *WLAN Parameters* tab for APs has several parameters that are not available to WBs and SAs and the *WLAN Parameters* tab for WBs and SAs has one additional parameter that is not available to APs. These parameters are clearly indicated in the description.



**Figure 5-19: WLAN Parameters Tab – Access Point**

The *WLAN Parameters* tab is comprised of the following components:

- ♦ **Hopping standard:** Displays the country specific hopping standard for which the device is configured. The hopping standard affects the number of hopping sequences that can be defined per hopping set.

- ◆ **Hopping Set:** This parameter is only configurable for APs. It is a read-only display for WBs and SAs. From the dropdown list, select the number of the hopping sets for the selected devices. Hopping sequences are grouped into a hopping set. Always use the same hopping set for all devices in the same site. Available values range from 1 to 3.
- ◆ **Hopping sequence:** This parameter is only configurable for APs. It is a read-only display for WBs and SAs. From the dropdown list, select the device's hopping sequence, which is a pre-defined series of channel that are used in a specific, pseudo-random order. It is recommended that when two or more APs are collocated in the same vicinity, a different hopping sequence is defined for each AP. When multiple APs are deployed in the same site, always select hopping sequences from the same hopping set to reduce the possibility of collisions in the WLAN.
- ◆ **Power Level:** Displays the output power level at which the device is transmitting at the antenna connector. The values can be either Low or High.
- ◆ **Use Prefix ESSID (AP only):** From the dropdown list, select whether to enable stations with partial ESSIDs to associate with the Access Point and adopt the complete ESSID upon association with the Access Point. The possible selections are On or Off.
- ◆ **Prefix ESSID (AP only):** Enter the prefix ESSID string to be used if the Use Prefix ESSID is enabled.
- ◆ **ESSID:** Enter the ESSID for the selected device. The ESSID identifies the WLAN, which prevents the unintentional merging of two collocated WLANs, since a station can only associate with an AP that has the identical ESSID. The ESSID can be a string of up to 32 case-sensitive printable ASCII characters.

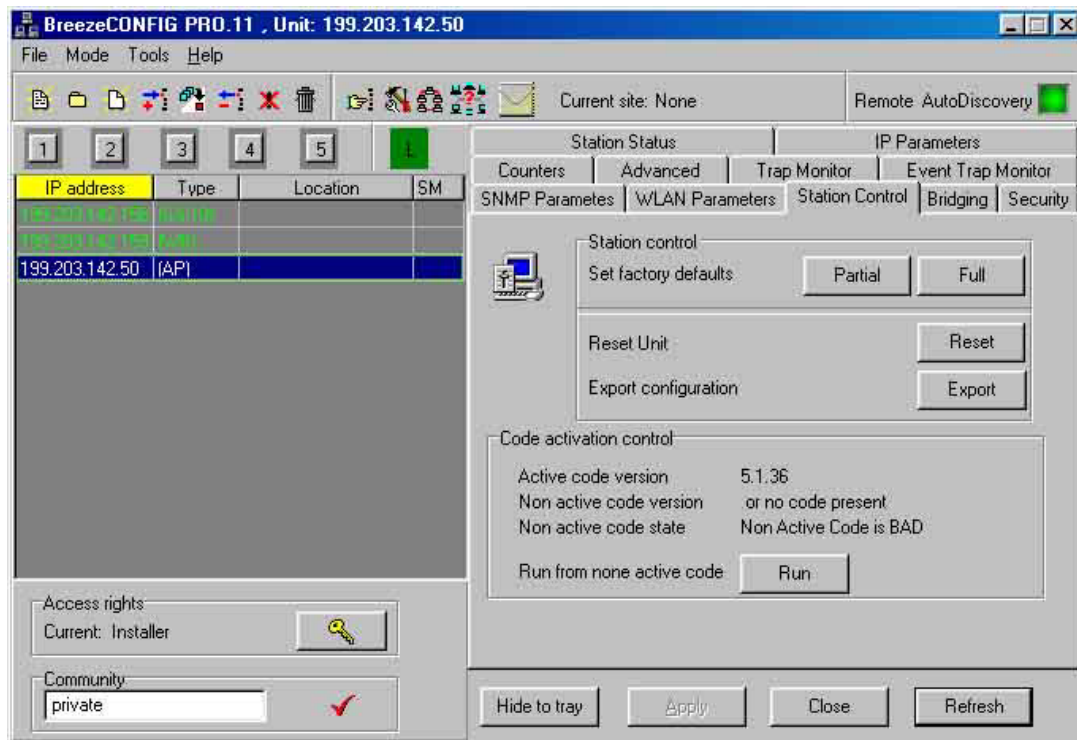
- ◆ **Maximum data rate:** From the dropdown list, select the maximum data rate for the selected device. The device automatically switches between available data rates depending on current network conditions. Depending on certain range/speed trade-offs, you may benefit from limiting the use of higher rates. The available values are 1 Mbps, 2 Mbps and 3 Mbps.
- ◆ **Mobility:** From the dropdown list, select the mobility status of the selected device. This enables the device to optimize its roaming algorithm depending on the device's mobility. Select from the following options:
  - ❖ **Stationary:** For stations that move less than 10km per hour. This is the default and generally the best selection.
  - ❖ **Portable:** For stations that move faster than 10km per hour and less than 30km per hour.
  - ❖ **Mobile:** For stations that move faster than 30km per hour.
- ◆ **Load sharing:** From the dropdown list, select whether stations should distribute themselves evenly among APs to optimize the traffic load between APs. This increases the aggregate throughput in collocated cells with multiple APs. The available selections are **On** or **Off**. All devices in the site should be configured to the same value.
- ◆ **Preferred AP (WB, SA only):** In the text box, enter the MAC address of the AP with which the selected device should associate. The device associates with the defined AP even if its signal is lower than other neighboring APs. The selected device only roams to another AP if it ceases to receive beacons from the preferred AP.

- ◆ **Transmit diversity:** When receiving, devices dynamically switch between optimal antennas. During transmission, the devices select the antenna prior to sending the transmission. Generally, the antenna last used successfully is selected first. In models with external antennas, in certain cases, only a single antenna is used. In these cases, the **Transmit Diversity** should be configured to transmit only from that single antenna. Similarly, models using a booster or an LNA only use a single antenna for transmission. The available values include **Both Antennas**, **Antenna No. 1** and **Antenna No. 2**.

## Station Control

The *Station Control* tab enables you to reset parameters to their factory default and manage the software versions of the selected device.

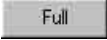
The *Station Control* tab for WBs and SAs is a read-only display that lists the active and non-active code versions for the selected device.



**Figure 5-20: Station Control Tab – Access Point**

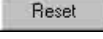
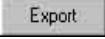

The *Station Control* tab is comprised of the following components:

- ◆ **Set factory defaults:** Reverts the system parameters to the original factory defaults, as follows.
  - ❖ Click **Partial** to revert all parameters to the factory default values except for those parameters that are necessary to ensure connectivity and enable management.

- ❖ Click  to revert all parameters to the selected set of factory default values.

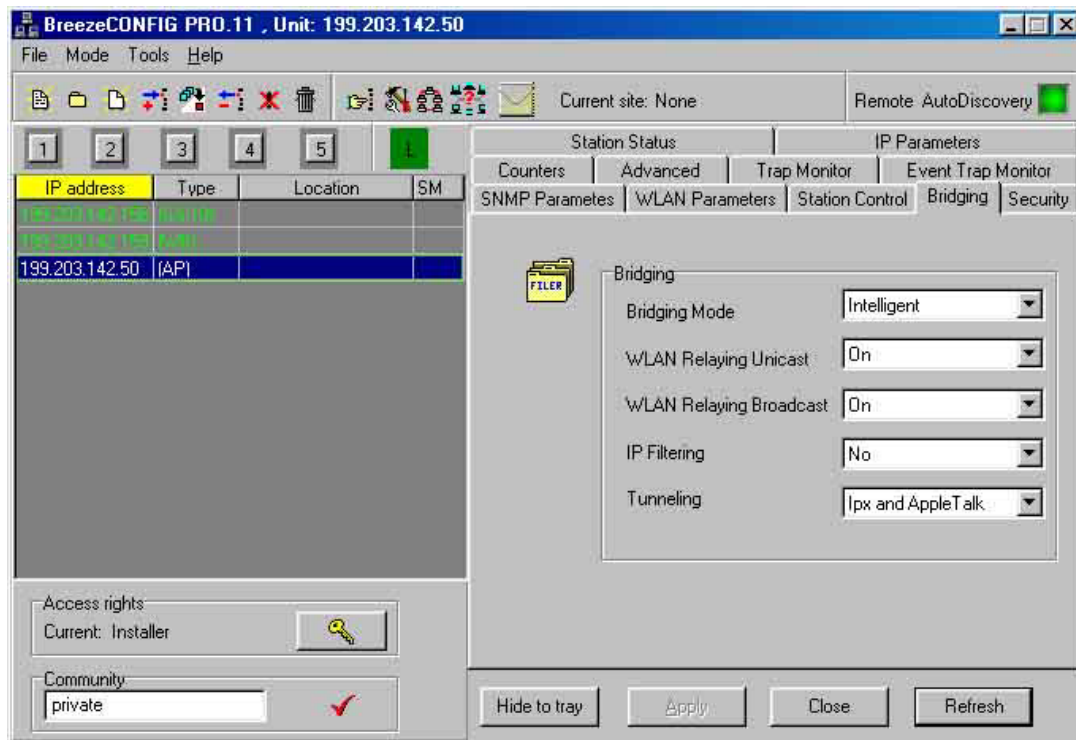
**NOTE:**

Clicking **Full** may cause you to lose connectivity to the device.

- ◆ **Reset Device:** Click  to reset the selected device and apply any modifications made to the system parameters.
- ◆ **Export configuration:** Click  to save the device's configuration as a BreezeNET configuration file, with the extension.Brz. The *Save As* window is displayed, enabling you to select a location for the file and to define a file name.
- ◆ **Code activation control:** The BreezeNET firmware comprises a two-code mechanism that enables you to swap back and forth between the two versions installed in the device. One version is designated as the Active code and the other is designated as the Non Active (Shadow) code.
  - ❖ **Active code version:** Displays the currently active SW version.
  - ❖ **Non active code version:** Displays the version of the device's shadow SW version.
  - ❖ **Non active code state:** Displays the status of the device's shadow SW version. The possible states are **GOOD** or **BAD**.
  - ❖ Click  to reset the device and activate the shadow version.

## Bridging (AP only)

The *Bridging* tab, which is only available to Access Points, enables you to define bridging mode, unicast and broadcast parameters. In addition, you can define parameters related to IP filtering and tunneling.



**Figure 5-21: Bridging Tab – Access Point**

The *Bridging* tab is comprised of the following components:

- ◆ **Bridging Mode:** From the dropdown list, select the device's bridging mode from the following option:
  - ❖ **Reject Unknown:** Packets are only transmitted to stations that the AP knows to exist in the Wireless LAN.

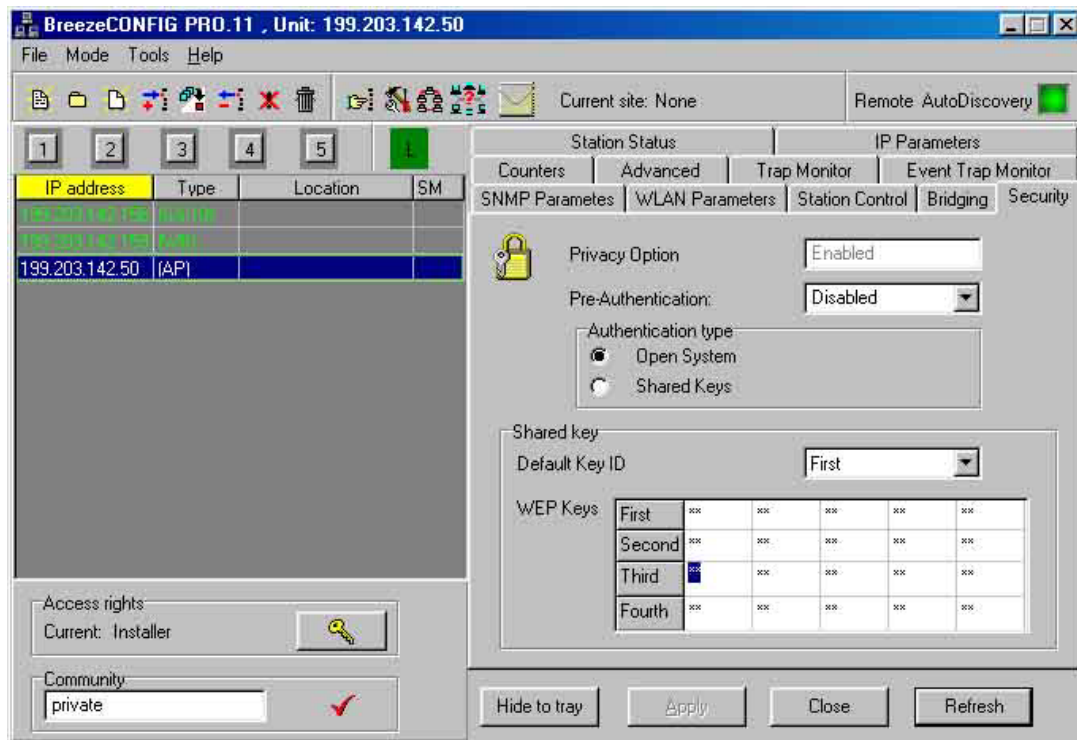


- ❖ **Forward Unknown:** All packets are transmitted except those sent to stations that the AP knows to exist on its wired Ethernet side.
- ❖ **Intelligent:** Select this option to cause the AP to enter a special bridging mode for a fixed amount of time whenever a WB roams into its area. This mode causes the AP to forward packets destined for the stations behind the WB-10 even though they are unknown. Afterward, the AP switches back to **Reject Unknown** bridging mode. This prevents the loss of packets destined for stations behind the Workgroup Bridge.
- ◆ **WLAN Relaying Unicast:** From the dropdown list, select whether to **enable** or **disable** the unicast relaying mechanism. If enabled, unicast packets originating from devices on the WLAN can be transmitted by the AP back to the WLAN devices. If disabled, these packets are not sent back to the WLAN even if they are intended for devices on the WLAN side. The available values are **On** or **Off**.
- ◆ **WLAN Relaying Broadcast:** From the dropdown list, select whether to **enable** or **disable** the broadcast relaying mechanism. If enabled, broadcast packets originating from devices on the WLAN are transmitted by the AP back to the WLAN devices, as well as to the wired Ethernet. If disabled, these packets are sent only to the local wired Ethernet and not back to the WLAN. The available values are **On** or **Off**.
- ◆ **IP Filtering:** From the dropdown list, select whether to enable IP filtering on the selected device. If enabled, the filter permits only IP traffic to pass through the WLAN. The available options are **Yes** or **No**.
- ◆ **Tunneling:** From the dropdown list, to ensure smooth communications, select the tunneling protocol option according to the protocols running over the network. The available options are **Ipx Only**, **AppleTalk Only**, **Ipx and AppleTalk** and **No**. All units must be configured with the same tunneling option.

## Security

Unauthorized wireless connection is prevented using the Wired Equivalent Privacy (WEP) algorithm defined in the IEEE 802.11 Wireless LAN standard. The WEP is based on the RSA's RC4 encryption algorithm.

The *Security* tab enables you to define WEP Keys to be used for authentication purposes.



**Figure 5-22: Security Tab**

The *Security* tab is comprised of the following components:

- ◆ **Privacy Option:** A read-only field that indicates whether the *Privacy Option* is **Enabled** or **Disabled**.

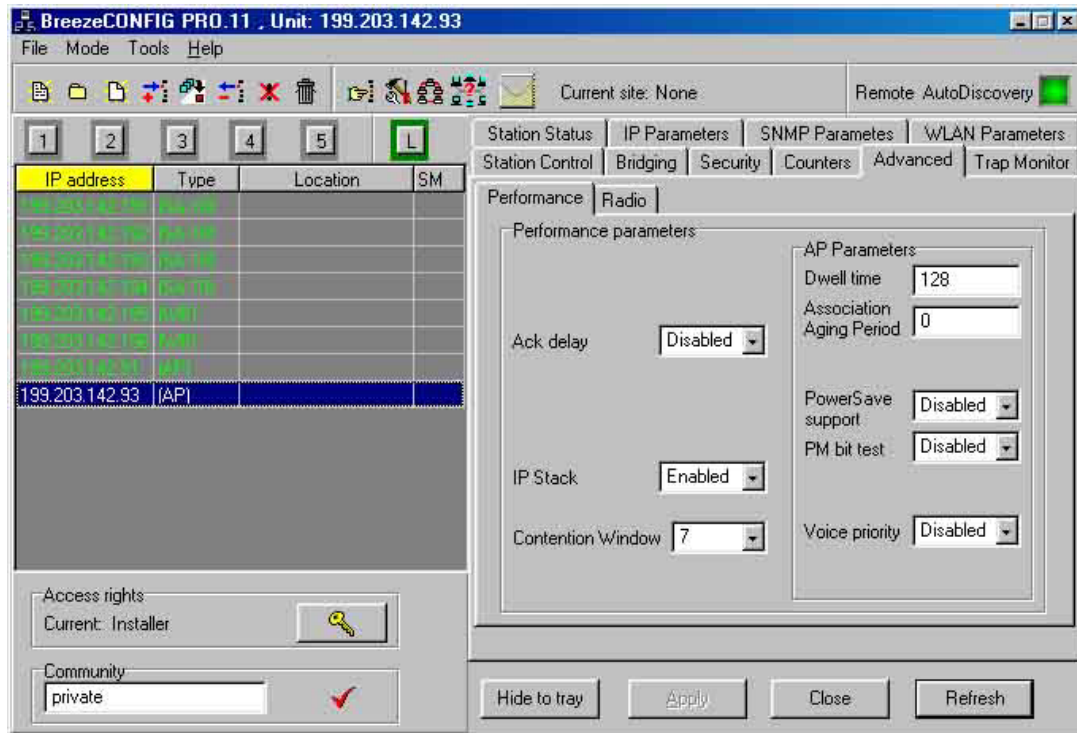
- ◆ **Pre-Authentication:** This parameter should be set to **Enabled** if there is a lot of roaming between APs in your network. The option must be configured the same for all Access Points and stations in the network.
- ◆ **Authentication type:** Mark the required option to select the operation mode of the device, from the following options:
  - ❖ **Open System:** A WB or SA configured to **Open System** can only associate with an AP also configured to **Open System**. In this case, the WEP algorithm is not used.
  - ❖ **Shared Key:** In this case, only WBs and SAs can only associate with APs configured to use the same WEP key.
- ◆ **Default Key ID:** From the dropdown list, select the WEP Key to be used for authentication purposes. The available values are **First**, **Second**, **Third** and **Fourth** and correspond to the applicable entries in the **WEP Key** table.
- ◆ **WEP Key:** To define the available WEP Keys to be used for authentication, select a row in the **WEP Key** table and enter the WEP Key, which is entered as 5 groups of two hexadecimal numbers per group.

## Advanced Parameters

The *Advanced* tab for APs includes two secondary tabs for *Performance* and *Radio* parameters. The *Advanced* tab for WB and SA devices includes a third tab for *Access* parameters.

## Performance

The *Advanced Performance* tab for Access Points comprises parameters that are not present on the *Advanced Performance* tab for WB and SA devices, which is clearly indicated in the description.



**Figure 5-23: Advanced Performance Tab – Access Point**

The *Advanced Performance* tab is comprised of the following components:

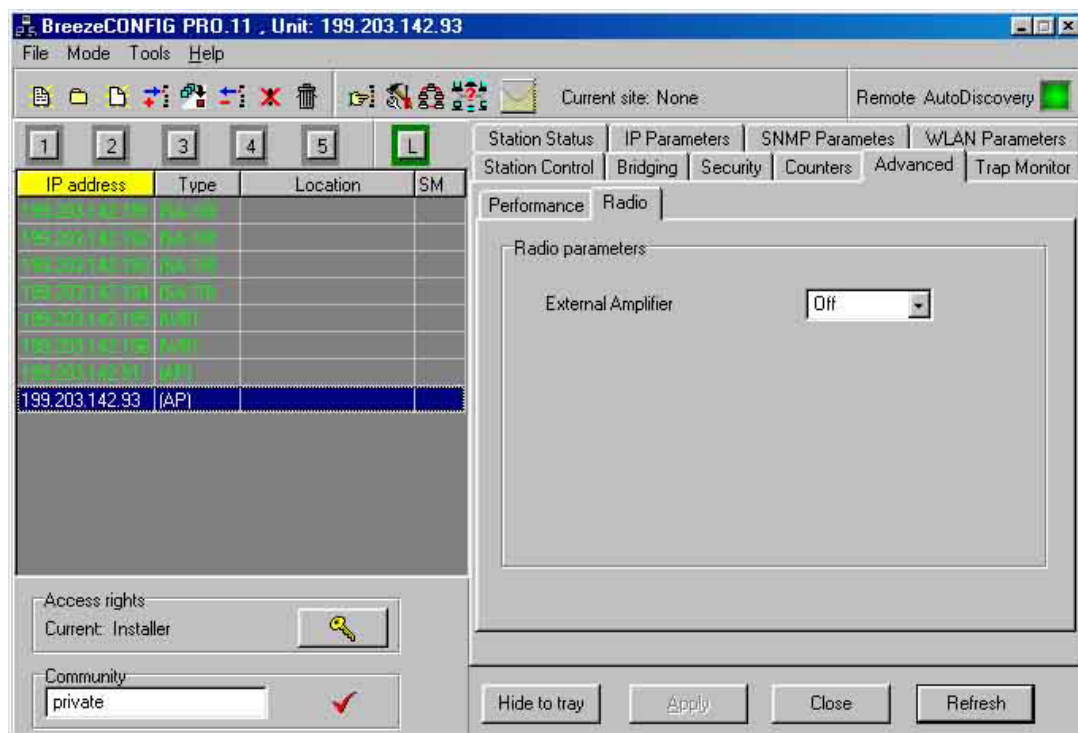
- ♦ **Ack Delay:** From the dropdown list, select whether to increase the range of the system. This should only be enabled for links above 20km. If enabled for a station, the **Ack Delay** must be enabled for the Access Point. The available values are **Enabled** or **Disabled**.

- ◆ **IP Stack:** From the dropdown list, select whether to enable the **IP Stack** option. When the IP stack is disabled, performance is improved. However, all IP management protocols are also disabled, including SNMP, TFTP, ICMP and DHCP. This means that the unit can no longer be remotely managed, including by the BreezeCONFIG PRO.11 configuration utility. The **IP Stack** can only be reset to **Enabled** with the Monitor program via the Monitor port. The available values are **Enabled** or **Disabled**.
- ◆ **Contention Window:** From the dropdown list, select the number to define the minimum contention window, which affects the calculation of the time that the device waits from the time it has concluded that there are no detectable transmissions from other devices before it attempts to transmit. The higher the number of hidden stations served by the same AP, the larger the value that should be set for this parameter. The available values are **7**, **15**, **31** and **63**.
- ◆ **Dwell Time (AP only):** Enter the amount of time spent on a radio channel before hopping to the next channel in the sequence. The available values range from **19** to **390** Kilo-microseconds.
- ◆ **Association Aging Period (AP only):** If the AP does not receive any message from a station for a period of time greater than the **Association Aging Period**, the AP assumes that the station is no longer associated with it and the station is removed from the APs associated stations database. The available values range from **30** to **180** minutes or **0** for no aging.
- ◆ **PowerSave support (AP only):** From the dropdown list, select whether to enable the **Powersave support**. The **PowerSave support** must be enabled if the AP serves at least one device, such as an SA-PCR, in which the **PowerSave support** is enabled. The available selections are **Enabled** and **Disabled**.

- ◆ **PM bit test (AP only):** From the dropdown list, select whether the AP supports the IEEE802.11 Power Save mode (when enabled) or Alvarion's proprietary Power Save mode (when disabled). The available selections are **Enabled** and **Disabled**
- ◆ **Voice Priority (AP only):** From the dropdown list, select whether to enable or disable the **Voice Priority** option. When enabled, the AP gives a higher priority to SpectraLink voice packets.

## Radio

The *Advanced Radio* tab is identical for all device types and enables you to define the **External Amplifier** parameter.



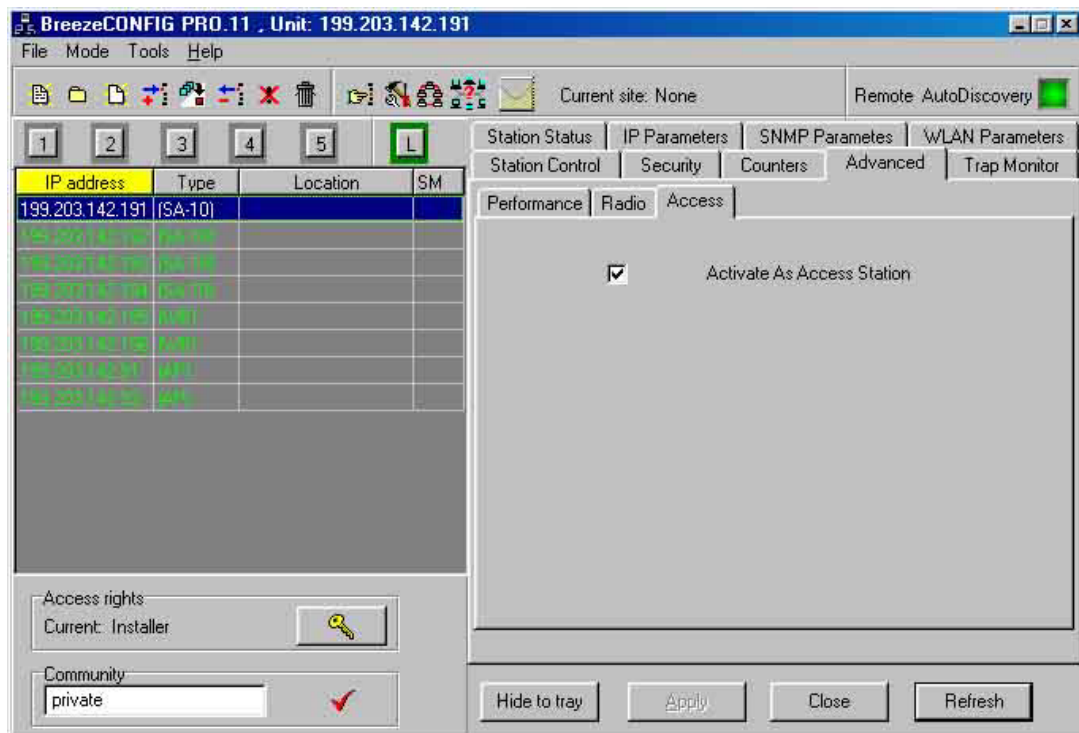
**Figure 5-24: Advanced Radio Tab**

The *Advanced Radio* tab is comprised of the following components:

- ♦ **External Amplifier:** From the dropdown list, set the **External Amplifier** to **On** when the unit is connected to an AMP2440 bi-directional amplifier or LNA-10 receive amplifier. The available selections are **On** or **Off**.

## Access (WB, SA Only)

The *Advanced Access* tab enables you to define to activate the selected device as an Access Point.



**Figure 5-25: Advanced Access Tab**

The *Advanced Access* tab is comprised of the following components:

- ◆ **Activate As Access Station:** Applicable to SA-10 devices only. Normally the SA-10 uses the MAC address of the connected device for association. This means that the SA-10 can only complete the association process once it has learned its MAC address. By marking the checkbox, the device operates like an Access Unit, using its own MAC address in the association process. It must be enabled whenever the connected device is a printer or any other device that does not have a MAC address.

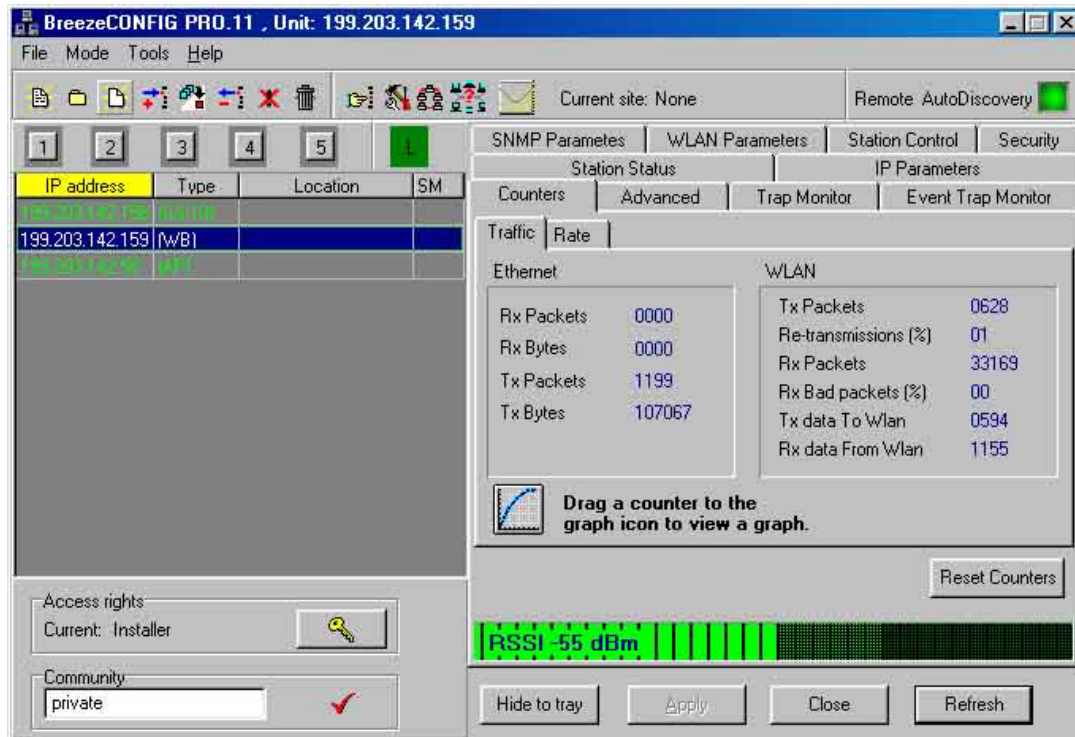
## Counters

The *Counters* tab enables you to view statistics about each device. The tab is comprised of the two secondary tabs, *Traffic* and *Rate*.



## Traffic Counters

The *Traffic Counters* tab displays information about the data received and transmitted to and from the selected device. The *Traffic Counters* tab for WB and SA devices includes an RSSI bar.



**Figure 5-26: Traffic Counters Tab – Workgroup Bridge**


The *Traffic Counters* tab is comprised of the following components:

- ◆ **Ethernet**

- ❖ **Rx Packets:** Total number of packets received from the Ethernet port.
- ❖ **Rx Bytes:** Total number of bytes received from the Ethernet port.

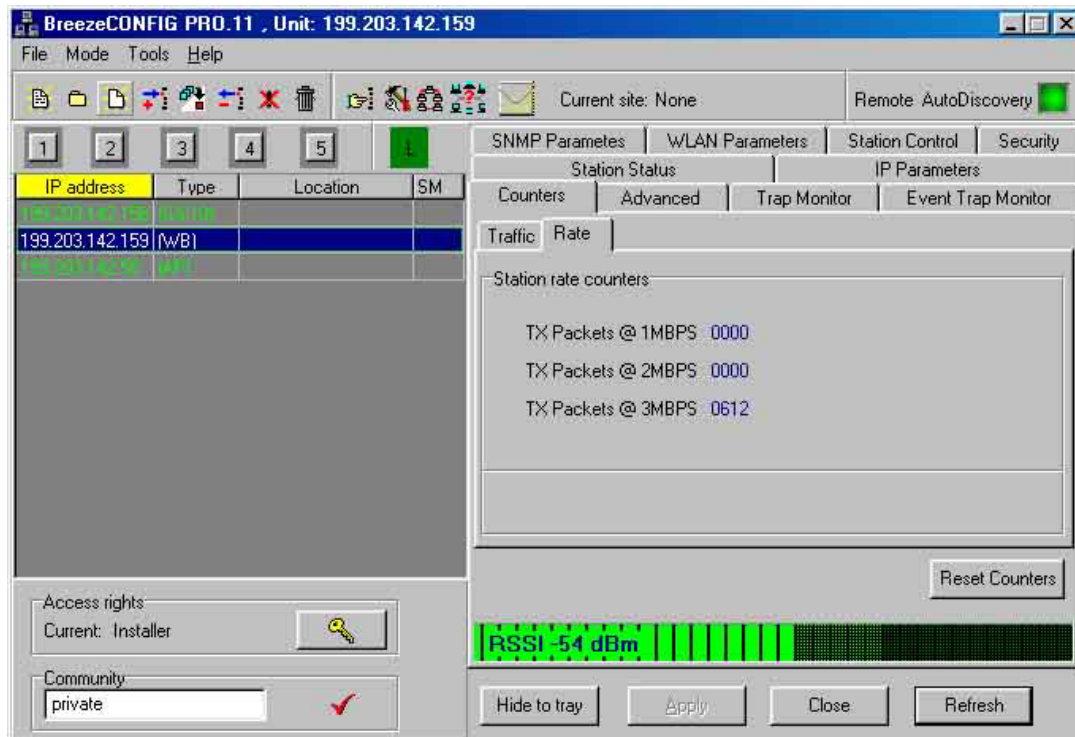
- ❖ **Tx Packets:** Total number of packets transmitted to the UTP port, including frames received from the Wireless LAN and frames generated by the device itself.
- ❖ **Tx Bytes:** Total number of bytes transmitted to the UTP port.

◆ **WLAN**

- ❖ **Tx Packets:** Total number of frames transmitted successfully. This includes beacons but does not include retransmissions.
- ❖ **Re-transmissions (%):** Total number of frames retransmitted as a percentage of the total number of transmitted frames.
- ❖ **Rx Packets:** The number of frames received from the wireless media, including data, control frames and beacons.
- ❖ **Rx Bad packets (%):** The percentage of packets received from the WLAN containing errors.
- ❖ **Tx data to Wlan:** Total number of data frames sent to the wireless media.
- ❖ **Rx data From Wlan:** Total number of data frames received from the wireless media.
- ❖ **RSSI Bar (WB and SA only):** Displays the devices signal strength.
- ❖ Click  to revert the counters to zero.

## Rate Counters

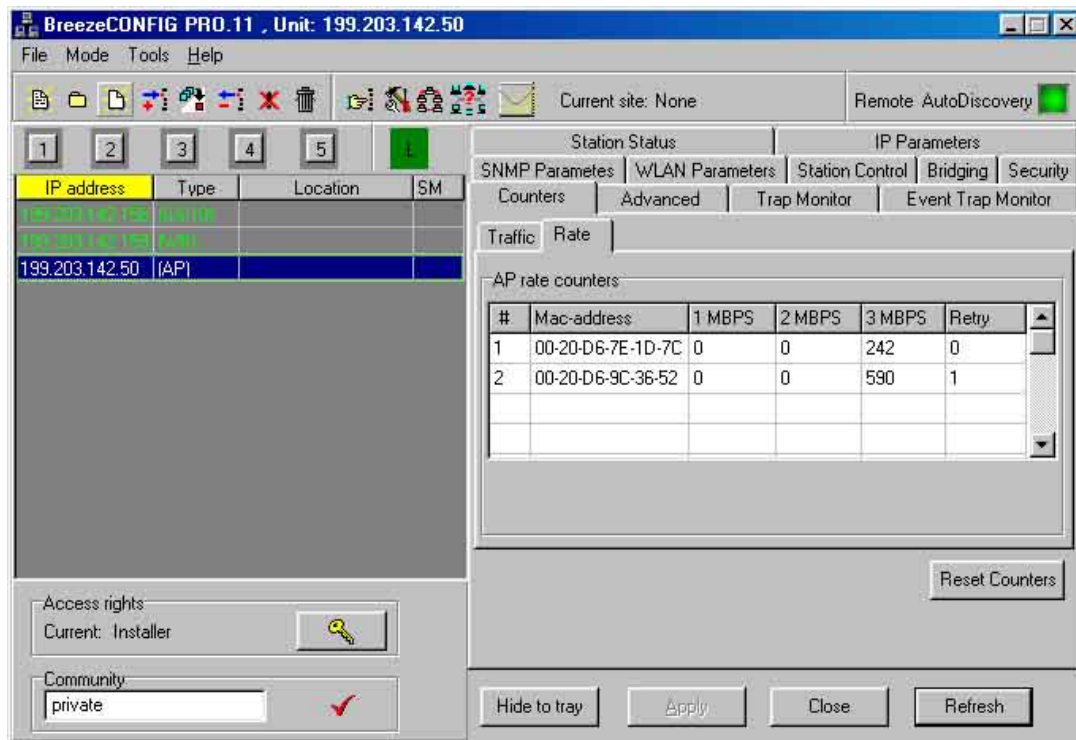
The *Per Rate Counters* tab displays information related to each data rate supported by the selected device. The *Rate Counters* tab differs completely between Access Points and Workgroup Bridges and Station Adapters. The WB and SA tab displays information regarding the transmitted frames at each data rate for selected device, whereas the Access Point's tab displays a table containing information on transmitted and retransmitted frames at each data rate for each device with which it is associated.



**Figure 5-27: Rate Counters Tab – Workgroup Bridge**

The *Rate* tab of the *Counters* tab for Workgroup Bridges is comprised of the following components:

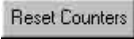
- ◆ **TX Packets @ <data rate>**: Displays the total number of frames transmitted by the selected device at the relevant data rate.
- ◆ Click **Reset Counters** to revert all statistics to zero.



**Figure 5-28: Rate Counters Tab – Access Point**

The *Rate* tab of the *Counters* tab for Access Points is comprised of a table that includes the following information for each associated device:

- ◆ **MAC Address**: The MAC address of the device.
- ◆ **1 MBPS, 2MBPS, 3 MBPS**: Displays the total number of frames transmitted by the AP to the selected device at the relevant data rate.

- ♦ **Retry:** Displays the total number of frames retransmitted to the selected device.
- ♦ Use the vertical scroll bar to review additional devices.
- ♦ Click  to revert all statistics to zero.

## Reading Trap Messages

The *Trap Monitor* tab displays SNMP trap messages and related information received from the device.

### Accessing Trap Messages

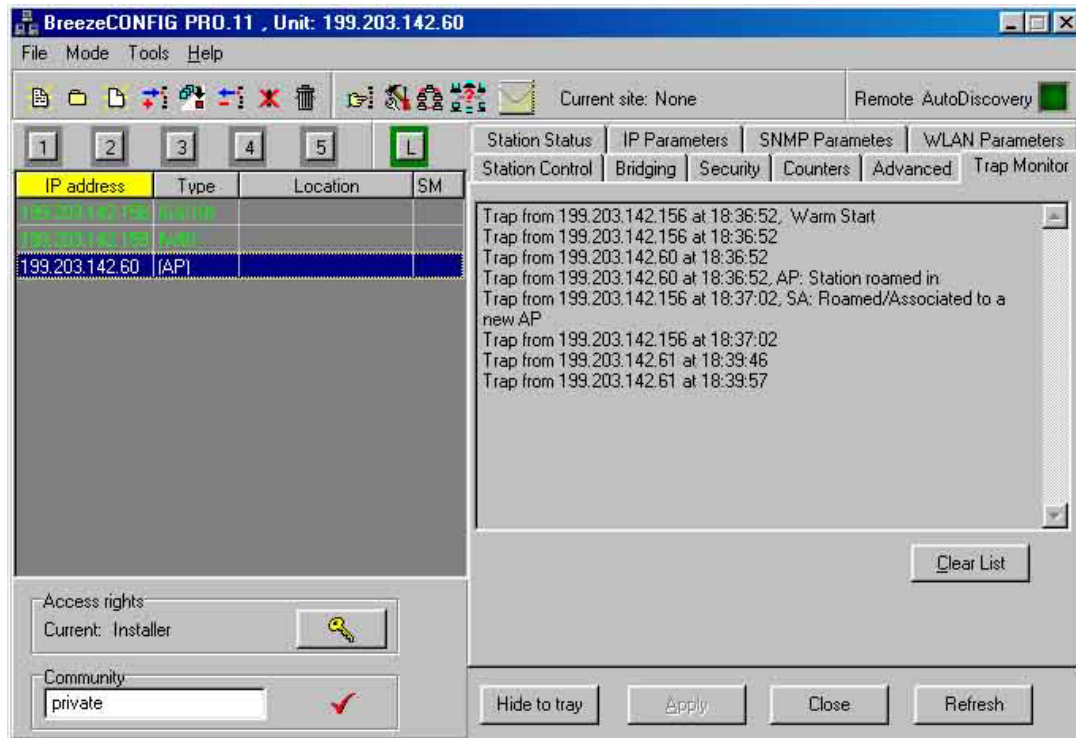
To receive trap messages several procedures must be undertaken as described in this section.

➤ **To access trap messages:**

1. Select the required device from the device list.
2. The IP address and trap community must be configured in the *Trap Table* of the *SNMP Parameters* tab, as described on page 5-41.
3. The **Trap Sending** option in the *SNMP Parameters* tab must be set to **Enabled**, as described on page 5-41.
4. These modifications must be applied and the device reset before trap messages are received.
5. To cause the *Trap Monitor* tab to be automatically displayed upon receiving a trap message, from the *Mode* menu, select **Trap quick view**.

## Trap Table

The *Trap Monitor* tab comprises a series of messages that pertain to the ongoing functioning of the devices.



**Figure 5-29: Trap Monitor Tab**

Each *Trap Monitor* messages is comprised of the following information:

- ◆ IP address of the device from which the trap originated.
- ◆ The date and time that the trap is received.
- ◆ Most messages include a description of the event that caused the trap to be sent.



# Chapter 6

## Planning and Installing Wireless LANs

### About This Chapter

All products in the BreezeNET PRO.11 series are available in several models: standard, D, and DE. The standard model is equipped with two integrated 2 dBi omni-directional antennas and is suitable for indoor, short-to-medium range installations. The D and DE models are equipped with two customized female connectors for use with a range of external antennas.

This chapter describes various possible system configurations, lists points to consider when performing indoor and outdoor installations, presents guidelines and restrictions regarding external antenna installation, and also describes antennas that are recommended to operate with BreezeNET PRO.11 units.

This chapter is comprised of the following sections:

- ♦ **System Configurations**, page 6-2, provides a series of possible configurations for deploying a wireless LAN.

- ♦ **Indoor Installation Considerations**, page 6-15, describes the various factors that must be considered in terms of site selection and ancillary equipment.
- ♦ **Outdoor Installation Considerations**, page 6-21, describes the various factors that must be considered in terms of site selection and equipment when installing the outdoor components.
- ♦ **Available Antennas and Antenna Kits**, page 6-38, describes the antenna and antenna kits available to operate with the system and describes all the factors that must be considered when selecting the optimal equipment.
- ♦ **Precautions**, page 6-41, describes certain equipment and personnel safety issues that must be considered with deploying the equipment.

## System Configurations

This chapter describes various wireless LAN configurations, and how to set them up:

- ♦ **Single Cell Configuration:** The wireless LAN consists of an Access Point and the wireless workstations with which it is associated.
- ♦ **Overlapping Cell Configuration:** The wireless LAN consists of two or more adjacent Access Points with slightly overlapping coverage.
- ♦ **Multicell Configuration:** The wireless LAN consists of several Access Points installed in the same location. This creates a common coverage area that increases aggregate throughput.
- ♦ **Multi-Hop Configuration:** The wireless LAN contains AP-WB pairs that extend the range of the wireless LAN.

Many wireless LANs contain several of these configurations at different points in the system. The Single Cell configuration is the most basic, and the other configurations build upon it.



## Single Cell Configuration

A basic BreezeNET cell consists of an Access Point and the wireless workstations with which it is associated. You can convert most workstations (e.g., PCs and X-Terminals) that are equipped with an Ethernet network interface card (NIC) to wireless workstations by connecting a BreezeNET SA-10 PRO.11 station adapter. You can convert most laptop computers with a PCMCIA slot into a wireless mobile station by using the SA-PCR PRO.11 PCMCIA card.

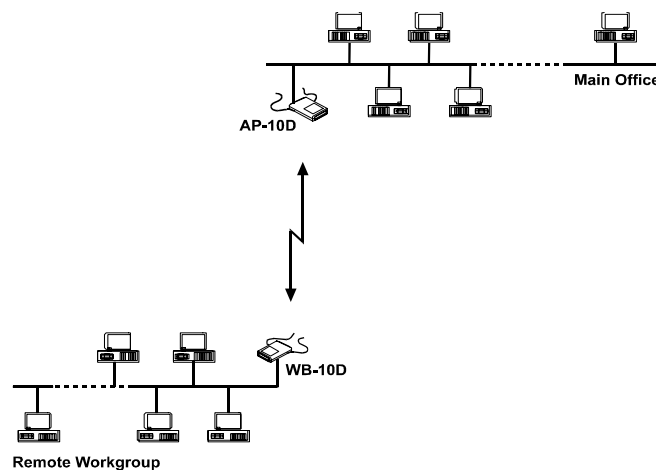
There are three types of Single Cell configurations:

- ◆ Point-to-Point
- ◆ Point-to-Multipoint
- ◆ Mobile Applications

Each configuration is explained in the following sections.

## Point-to-Point

The figure below illustrates the point-to-point configuration.



**Figure 6-1: Point-to-Point Configuration/  
Connecting Remote Offices to Main Office Network**

Point-to-Point installations require directional antennas at either end of the link. To select the best antenna for a specific application, consider the following factors:

- ◆ Distance between sites
- ◆ Required throughput
- ◆ Clearance between sites
- ◆ Cable length.

Refer to *Using Outdoor Range Tables*, on page 6-27, to determine the best combination of antennas for your application.

## Point-to-Multipoint

Point-to-Multipoint applications consist of one or more APs at the central site and several remote stations and bridges (SA-10, SA-40, WB-10). In this configuration, use an Omni-6 antenna with the Access Point for its 360° radiation pattern. In the United States, the Omni-7.2 antenna (which also has a 360° radiation pattern but has a wider range) can also be used. The Omni-7.2 antenna comes with a 20ft. low loss cable and a mast mount bracket for rooftop installations.

The remote units should use directional antennas aimed toward the AP's antenna(s).

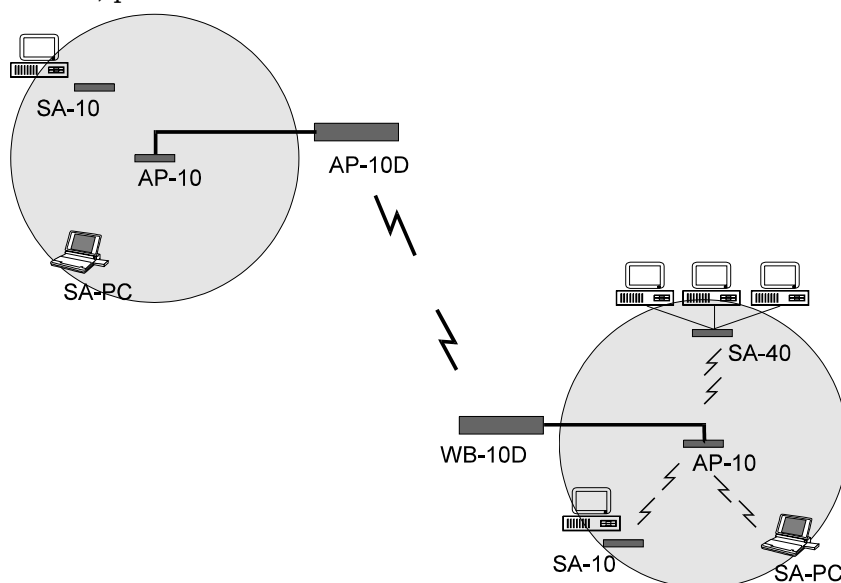
## Mobile Applications

In mobile applications, station orientation changes continuously. To maintain connectivity throughout the entire coverage area, most mobile applications require omni-directional antennas for both Access Points and wireless stations. In a motor vehicle, for example, you can install an SA-10 in the cabin, and mount the antennas (in most cases an Omni-6) on the roof.

## Extending the LAN with WLAN Bridging

Figure 6-2 demonstrates how the WB-10 can be used to extend a regular network with a wireless link.

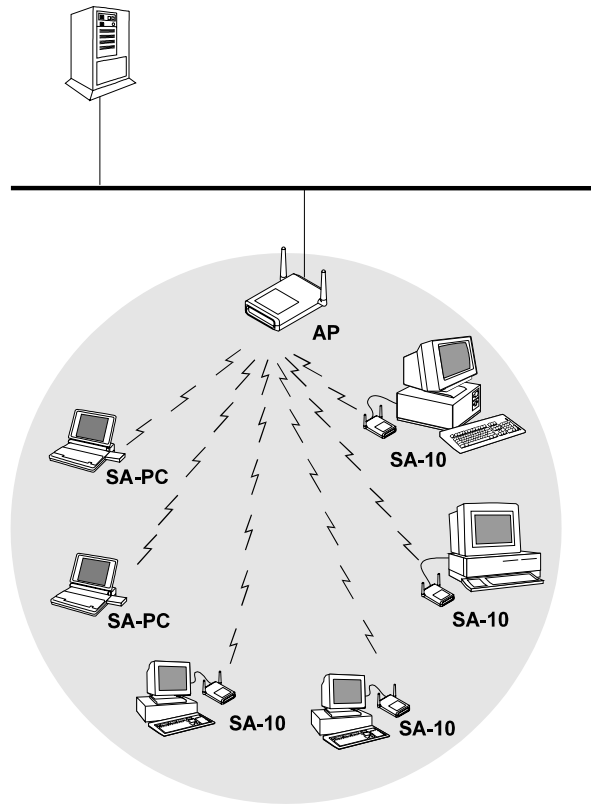
The WB-10 PRO.11 also enables connectivity between a wireless LAN and individual workstations or workgroups located outside the LAN. The WB-10 PRO.11 enables these wireless stations in its coverage area to communicate with the wireless LAN and gain access to its network resources such as file servers, printers and shared databases.



**Figure 6-2: Wireless Bridging Between Two or More Wireless LAN Segments**

## Setting up a Single BreezeNET Cell

The figure below illustrates how to deploy a single BreezeNET cell.



**Figure 6-3: Single Cell Configuration**

1. Install the Access Point (refer to Chapter 2 for installation instructions). Be sure to position the Access Point as high as possible.

**NOTE:**

It is not necessary at this point to connect the Access Point to an Ethernet backbone, since Access Points continuously transmit signals (beacon frames) whether they are connected to an Ethernet backbone or not.

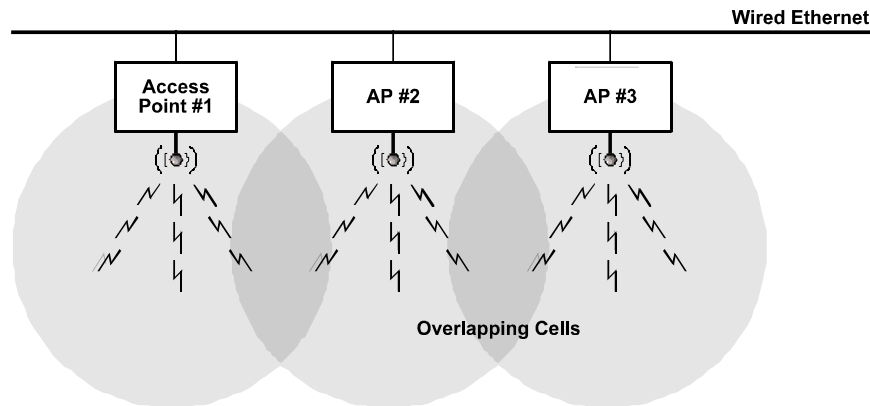
2. Install a Station Adapter (refer to Chapter 2 for installation instructions) or SA-PCR card (refer to Chapter 4 for installation instructions).
3. Check the Station Adapter front panel LED indicators, or the Site Survey application of the SA-PCR card to check signal strength.
4. Make any necessary adjustments, for example:
  - ♦ Adjust the antennas
  - ♦ Adjust the location of the Station Adapter
  - ♦ Adjust the location of the Access Point
5. Proceed to setup the other workstations.

## Overlapping Cell Configuration System Configurations

When two adjacent Access Points are positioned close enough to each other, a part of the coverage area of Access Point #1 overlaps that of Access Point #2. This overlapping area has two very important attributes:

- ♦ Any workstation situated in the overlapping area can associate and communicate with either Access Point #1 or Access Point #2.

- ◆ Any workstation can move seamlessly through the overlapping coverage areas without losing its network connection. This attribute is called *Seamless Roaming*.



**Figure 6-4: Three Overlapping Cells**

- **To set up overlapping BreezeNET cells:**
- 1.** Install an Access Point (refer to Chapter 2 for installation instructions). Be sure to position the Access Point at the highest point possible.
  - 2.** Install the second Access Point so that the two are positioned closer together than the prescribed distance (as listed in *Cell Size*, on page 6-20).
  - 3.** To enable roaming, configure all Access Points and stations adapters to the same ESSID.
  - 4.** To improve collocation and performance, configure all Access Points to different hopping sequences of the same hopping set.
  - 5.** Install a Station Adapter or SA-PCR card on a workstation.
  - 6.** Position the wireless workstation at approximately equal distances from the two Access Points.

- 7.** Temporarily disconnect the first Access Point from the power supply. Verify radio signal reception from the first Access Point. View the LED indicators of the front panel of the Station Adapter, or the Site Survey application of the SA-PCR card, to check the signal strength of the first Access Point.
- 8.** Disconnect the second Access Point from the power supply and re-connect the first Access Point. View the LED indicators of the front panel of the station adapter, or the Site Survey application of the SA-PCR card, to check the signal strength of the second Access Point.
- 9.** If necessary, adjust the distance between the Access Points so the coverage areas overlap.
- 10.** Continue setting up overlapping cells until the required area is covered.

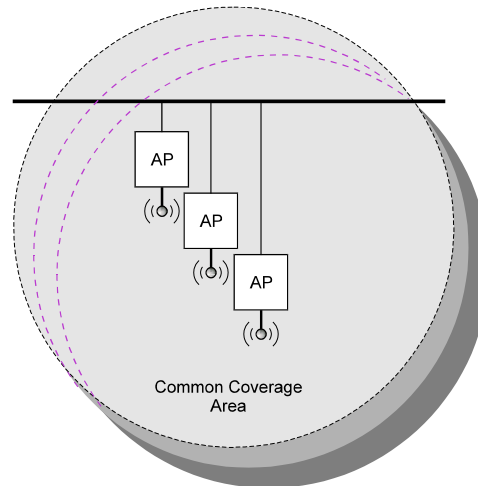
**NOTE:**

It is not necessary at this point to connect the Access Points to an Ethernet backbone, since Access Points continuously transmit signals (beacon frames) whether they are connected to an Ethernet backbone or not.



## Multicell Configuration

Areas congested by many users and a heavy traffic load may require a multicell structure. In a multicell structure, several Access Points are installed in the same location. Each Access Point has the same coverage area, thereby creating a common coverage area that increases aggregate throughput. Any workstation in the overlapping area can associate and communicate with any Access Point covering that area.



**Figure 6-5: Multicell Configuration**

➤ **To set up a BreezeNET multicell:**

1. Calculate the required number of Access Points as follows: multiply the number of active users by the required throughput per user, and divide the result by 1.5Mbps (which is the net throughput supported by collocated Access Points). Consider the example of five active stations, each requiring 0.5 Mbps throughput. The calculation is  $(5 \times .5) / 1.5 = 1.6$ . Two Access Points should be used. This method is accurate only for the first few Access Points.

2. The aggregate throughput of the common coverage area is equal to the number of co-located Access Points multiplied by the throughput of each individual Access Point, minus a certain amount of degradation caused by the interference among the different Access Points.
3. Install several Access Points in the same location a few meters from each other so they cover the same area. Be sure to position the Access Points at the highest points possible.
4. To enable roaming and redundancy, configure all Access Points and stations adapters to the same ESSID.
5. To improve collocation and performance, configure all Access Points to different hopping sequences of the same hopping set.
6. Install Station Adapters or SA-PCR cards on workstations.
7. Make sure that the Load Sharing option is activated. Stations automatically associate with an Access Point that is less loaded and provides better signal quality.

**NOTE:**

It is not necessary at this point to connect the Access Points to an Ethernet backbone, since Access Points continuously transmit signals (beacon frames) whether they are connected to an Ethernet backbone or not.

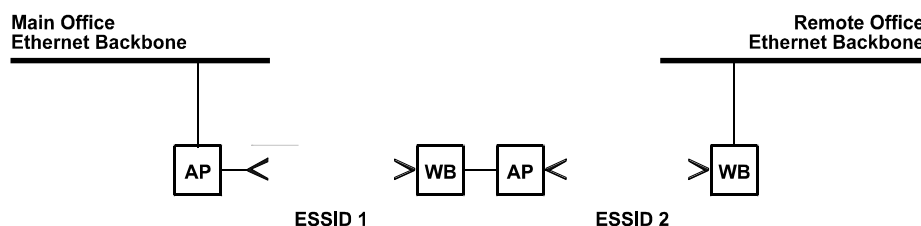
## Multi-Hop Configuration (Relay)

When you need to connect two sites and no line-of-sight exists between them, an AP-WB pair can be positioned at a third location where line-of-sight exists with each of the original locations. This third location then acts as a relay point.

In areas where a wired LAN backbone is not available, another AP can be added to the AP-WB relay to distribute a wireless backbone. In this manner, the range of a wireless system can be extended.

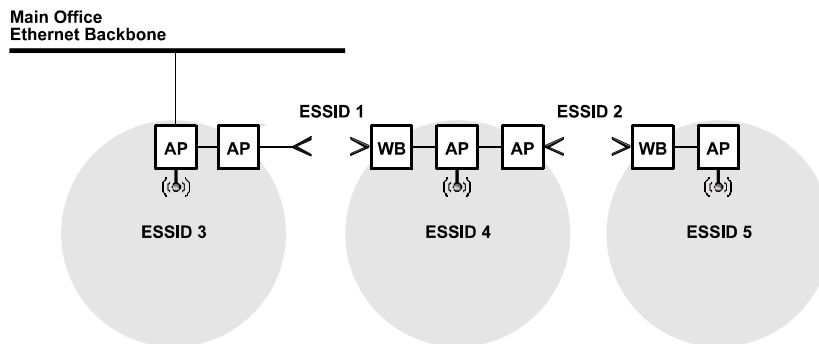
➤ **To set up a BreezeNET multi-hop cell:**

1. Install an AP at the main office (refer to Chapter 2 for installation instructions).
2. Install a WB at the remote site.
3. Install an AP-WB pair in a high location that has a clear line of sight to both the main office and the remote site. Many AP-WB pairs can form a chain.
4. When an AP and WB communicate over the wireless LAN, set them both to the same ESSID. For example, set the AP of the main office and the WB of the first AP-WB relay pair to the same ESSID. Also, set the AP of the last AP-WB relay and the WB of the remote site to the same ESSID; this ESSID should be different from the first ESSID.
5. Another option is to use one ESSID, and to set the Preferred AP parameter of each WB to its paired AP (refer to *Wireless LAN (WLAN) Parameters*, on page 3-16). This option enables stations to roam between the sites.
6. As previously described, make sure that the hopping sequence of the Access Points is different.



**Figure 6-6: Multi-Hop Configuration**

7. If required, an additional AP can be added at the main office and remote site, and between each AP-WB pair to provide wireless LANs at those points (see Figure 6-7).

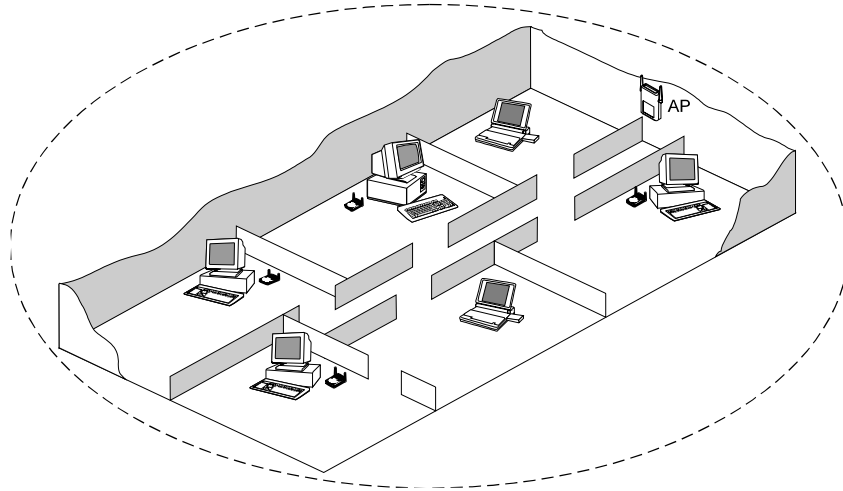


**Figure 6-7: Advanced Multihop Configuration**

8. Install Station Adapters or SA-PCR cards on workstations (refer to Chapter 2).

# Indoor Installation Considerations

This section describes various considerations that must be taken into account when planning an indoor installation. This includes site selection, antenna diversity, antenna polarization, construction materials and cell size.



**Figure 6-8: BreezeNET LAN in a Typical Office Environment**

## Site Selection Factors

BreezeNET PRO.11 wireless LAN products are robust, trouble-free units, designed to operate efficiently under a wide range of conditions. The following guidelines are provided to help you position the units to ensure optimum coverage and operation of the wireless LAN.

## **Metal Furniture**

Position the units clear of metal furniture and away from moving objects such as metal fans or doors.

## **Microwave Ovens**

For best performance, position the units clear of radiation sources that emit in the 2.4 GHz frequency band, such as microwave ovens.

## **Antennas**

Make sure the antennas are extended upward vertically in relation to the floor. For models with external antennas, connect the external antennas and RF cable.

## **Heat Sources**

Keep the units well away from sources of heat, such as radiators and air-conditioners

## **Site Selection for Access Points**

When positioning Access Points, take into account the following additional considerations.

### ***Height***

Install the Access Point at least 1.5m above the floor, clear of any high office partitions or tall pieces of furniture in the coverage area. The Access Point can be placed on a high shelf, or can be attached to the ceiling or a wall using a mounting bracket.

## **Central Location**

Install the Access Point in a central location in the intended coverage area. Optimal positions include:

- ♦ In the center of a large room.
- ♦ In the center of a corridor.
- ♦ At the intersection of two corridors.

Many modern buildings have partitions constructed of metal or containing metal components. We recommend that you install the Access Points on the corridor ceilings. The radio waves propagated by the BreezeNET PRO.11 LAN are reflected along the metal partitions and enter the offices through the doors or glass sections.

## **Antennas for Indoor Applications**

For most indoor applications, the best choice is the standard unit equipped with its integrated 2dBi antennas. The units are small, easy to install and cover a large area.

In some installations, it is required to install the unit and antenna separately. In such instances, use the AP-10D with the omni-6 antenna kit (6dbi omni-directional antenna with 3 meter RG-58 cable). In the USA (FCC regulated) and in non-regulated countries, the omni-6 comes with a shorter antenna cable, extending the coverage area.

The Uni-8.5 is also useful in indoor applications. It is very small and easily wall-mounted, but its radiation pattern is limited (75°).

Alvarion recommends that, for indoor applications, you use two antennas per unit to utilize the diversity gain of the system.

## Antenna Diversity

In applications where no multipath propagation is expected, a single antenna is sufficient to ensure good performance levels. However, in cases where multipath propagation exists, Alvarion recommends that two antennas be used. This takes advantage of space diversity capabilities. By using two antennas per unit, the system can select the best antenna on a per-packet basis (every several milliseconds).

Multipath propagation is to be expected when there are potential reflectors between the main and remote sites. These reflectors may be buildings or moving objects such as airplanes and motor vehicles. If this is the case, the radio signal does not travel in a straight line, but is reflected or deflected off of the object, creating multiple propagation paths.

When installing a single antenna, modify the **Transmit Diversity** option to either antenna 1 or antenna 2, according to the antenna being used (refer to *Wireless LAN (WLAN) Parameters*, on page 3-16).

## Antenna Polarization

Antenna polarization must be the same at either end of the link. In most applications, the preferred orientation is vertical polarization. Above-ground propagation of the signal is better when it is polarized vertically. To verify antenna polarization, refer to the assembly instructions supplied with the antenna set.



## Construction Materials

A cell's coverage area is affected by the construction materials of the walls, partitions, ceilings, floors and the furnishings of the cell. Due to their intrinsic nature, these materials may cause radio signal loss:

- ◆ Metal objects reflect radio signals. They do not let the signals pass through.
- ◆ Wood, glass, plastic and brick reflect part of the radio signals and allow part of the radio signals to pass through.
- ◆ Water and objects with high moisture content absorb a large part of the radio signals.

Use the following table as a guideline to predict the effects of different materials.

**Table 6-1: Signal Loss Chart**

<b>Obstruction</b>	<b>Additional Loss (dB)</b>	<b>Effective Range</b>	<b>Approx. Range</b>
Open Space	0dB	100%	1000ft. (300m)
Window (non-metallic tint)	3dB	70%	700ft. (215m)
Window (metallic tint)	5-8dB	50%	500ft. (150m)
Light Wall (dry wall)	5-8dB	50%	500ft. (150m)
Medium Wall (wood)	10dB	30%	300ft. (100m)
Heavy Wall (solid core 6")	15-20dB	15%	150ft. (50m)
Very Heavy Wall (solid core 12")	20-25dB	10%	100ft. (30m)
Floor/Ceiling (solid core)	15-20dB	15%	150ft. (50m)
Floor/Ceiling (heavy solid core)	20-25dB	10%	100ft. (30m)

**NOTE:**

Take stairwells and elevator shafts into consideration when positioning Access Points. There is no way to quantify the loss associated with these obstructions; however they do have an effect on the signal.

## Cell Size

Cell size is determined by the maximum possible distance between the Access Point and the Station Adapter. This distance varies according to the building floor plan and the nature of that environment. There are several general categories:

### Open Indoor Areas

Open office areas with no partitioning and no obstacles between the Access Point and the BreezeNET workstation.

The suggested maximum distance between Access Point and workstation:

Standard AP-10	200m (600 ft.)
PRO.11	

### Semi-Open Indoor Areas

Open-plan offices partitioned into individual workspaces, factory floor areas, warehouses, etc.

The suggested maximum distance between Access Point and workstation:

Standard AP-10	PRO.11	100m (300 ft.)
----------------	--------	----------------

## Closed Indoor Areas

A floor divided into individual offices by concrete, masonry or sheet-rock walls. A house is also a closed indoor area.

The suggested maximum distance between Access Point and workstation:

Standard AP-10 PRO.11      50m (150 ft.)

# Outdoor Installation Considerations

This section describes various considerations to take into account when planning an outdoor installation including site selection, antenna alignment, antenna diversity, antenna polarization, antenna seal, and cell size.

## Site Selection Factors

When selecting a location for external antennas, remember to take into consideration the following guidelines:

- ◆ Minimum distance between sites
- ◆ Maximum height above the ground
- ◆ Maximum line of sight clearance
- ◆ Maximum separation between antennas (diversity option)

## Path of Clearest Propagation

A propagation path is the path that signals traverse between the antennas of any two bridges. The “line” between two antenna sites is an imaginary straight line, which may be drawn between the two antennas. Any obstacles in the path of the “line” degrade the propagation path. The best propagation path is, therefore, a clear line of sight with good clearance between the “line” and any physical obstacle.

## Physical Obstacles

Any physical object in the path between two bridges can cause signal attenuation. Common obstructions are buildings and trees. If a bridge’s antenna is installed indoors, the walls and/or windows between the two sites are physical obstructions. If the antenna is positioned outdoors, any buildings or other physical structure such as trees, mountains or other natural geographic features higher than the antenna and situated in the path between the two sites can constitute obstructions.

Install indoor antennas as close as possible to a window (or wall if a window is not accessible) facing the required direction. Avoid metal obstacles such as metal window frames or metal film anti-glare windows in the transmission path. Install outdoor antennas high enough to avoid any obstacles, which may block the signal.

## Minimal Path Loss

Path loss is determined mainly by several factors:

- ◆ **Distance between Sites:** Path loss is lower and system performance better when distances between sites are shorter.
- ◆ **Clearance:** Path loss is minimized when there is a clear line of sight. The number, location, size, and makeup of obstacles determine their contribution to path loss.

- ♦ **Antenna Height:** Path loss is lower when antennas are positioned higher. Antenna height is the distance from the imaginary line connecting the antennas at the two sites to “ground” level. “Ground” level in an open area is the actual ground. In dense urban areas, “ground” level is the average height of the buildings between the antenna sites.

## Rooftop Installation

### **WARNING:**

Rooftop antenna installations are extremely dangerous! Incorrect installation may result in death, serious injury and/or damage. Such installations should be performed by professional antenna installers only!

Rooftop installations offer several advantages:

- ♦ Increased antenna range.
- ♦ Fewer obstacles in path.
- ♦ Improved performance due to greater height.
- ♦ Reduced multipath problems.

## Antennas for Outdoor Applications

The BreezeNET PRO.11 series can be used in point-to-point or point-to-multipoint configurations.

### Point-to-Point

A point-to-point link is based on the use of one Access Point with external antennas (AP-10D or AP-10DE) and one adapter (SA-10/40D, WB-10D or WB-10DE). The AP and the WB must be equipped with one or two directional antennas. The necessary antenna gain depends on the required range and performance.

## Point-to-Multipoint

Setting up a point-to-multipoint link requires the use of an AP-10D equipped with omni-directional antennas and a remote WB-10D (or SA-10/40D) equipped with high-gain directional antennas.

## Antenna Alignment

Low gain antennas do not require alignment due to their very wide radiation pattern. High gain antennas have a narrow beamwidth necessitating an alignment procedure in order to optimize the link.

Check antenna alignment by using the LED indicators on the front panel of whichever adapter is used in the link (WB-10D or SA-10/40D). These LED indicators provide indication of reception quality.

### ➤ To perform antenna alignment:

1. Assemble antennas according to the assembly instructions included with the antenna set.
2. Mount the antennas as high as possible.
3. Connect the coaxial cable to the AP at the main site.
4. Connect the coaxial cable to the WB (or SA) at the remote site.
5. Power on the AP and the WB (or SA).
6. Synchronize the units by aligning the antennas manually until the WLNK indicator LED on the front panel of the wireless Bridge and/or Station Adapter illuminates.
7. Align antennas at the main and remote sites until maximum signal quality is obtained. (Check QLT LEDs on the front panel of the Station Adapter and the wireless Bridge.)

If the received signal quality is lower than expected for this antenna/range combination, change antenna height and verify RF cables connections.

## Antenna Diversity

In applications where no multipath propagation is expected, a single antenna is sufficient to ensure good performance levels. However, in cases where multipath propagation exists, Alvarion recommends that two antennas be used. This takes advantage of space diversity capabilities. By using two antennas per unit, the system can select the best antenna on a per-packet basis (every several milliseconds).

Multipath propagation is to be expected when there are potential reflectors between the main and remote sites. These reflectors may be buildings or moving objects such as airplanes and motor vehicles. If this is the case, the radio signal does not travel in a straight line, but is reflected or deflected off of the object, creating multiple propagation paths.

When installing a single antenna, modify the **transmit diversity** option to either antenna 1 or antenna 2, according to the antenna being used (refer to *Wireless LAN (WLAN) Parameters*, on page 3-16).

## Antenna Polarization

Antenna polarization must be the same at either end of the link. In most applications, the preferred orientation is vertical polarization. Above-ground propagation of the signal is better when it is polarized vertically. To verify antenna polarization, refer to the assembly instructions supplied with the antenna set.

## Antenna Seal

When using outdoor antennas, you must seal the antenna connectors against rain. Otherwise the antennas are not suitable for use in outdoor installations.

## Cell Size

Cell size is determined by the maximum possible distance between the Access Point and the Station Adapter, usually related to point-to-multipoint installations using external antennas. For open outdoor areas with an unobstructed line of sight between the Access Point and the BreezeNET PRO.11 workstation, the suggested maximum distance between Access Point and workstation is:

Standard AP-10 PRO.11      700m (2000 ft.)

## Link Distance

Link distance is the maximum distance between the AP and the station adapter, usually related to point-to-point installations using external antennas. For open outdoor areas with an unobstructed line of sight between the Access Point and the wireless bridge, the suggested maximum distance is:

Unit	USA	Europe
AP-10D PRO.11 with external antennas	up to 10Km (7 miles)	up to 2.5Km in Europe
AP-10DE PRO.11 with external antennas	—	up to 5Km in Europe

**NOTE:**

The maximum distance of 10Km/7 miles is achieved using 24 dBi antennas. The maximum distance of 2.5Km is achieved using 18 dBi antennas.

For range tables, refer to *Using Outdoor Range Tables*, on page 6-27.



## Using Outdoor Range Tables

Outdoor installations must have a clear line-of-sight. Solid obstacles such as buildings or hills prevent the establishment of a link. Partial obstacles such as trees or traffic can reduce range. Extending coaxial cables can cause an increase in assembly signal loss and a reduction in range.

The ranges in the following tables are attained under good propagating conditions when using the standard cables supplied in the antenna set. Actual ranges may vary due to specific multipath and interference conditions.

For specific range guidelines and information about extending cables, consult your local dealer or Alvarion central offices.

Ranges are subject to change without notice.

## FCC Outdoor Range Tables (USA)

The following tables are compliant with FCC regulations.

**Table 6-2: BreezeNET USA/FCC Range Table - 1Mbps**

Ant. type		Omni-2	Omni-6	Omni-7	Uni-8.5	Uni-11	Uni-13	Uni-16	Uni-18	Uni-24
	Asmb gain	2 dBi	5 dBi	6 dBi	6.5 dBi	9 dBi	11 dBi	14 dBi	15 dBi	19 dBi
Omni-2	2 dBi	2500 ft	3800 ft	3900 ft	4000 ft	1.0 mi	1.2 mi	1.4 mi	1.5 mi	1.9 mi
Omni-6	5 dBi	3800 ft	4300 ft	4600 ft	4800 ft	1.2 mi	1.5 mi	1.7 mi	1.8 mi	2.2 mi
Omni-7	6 dBi	3900 ft	4600 ft	4800 ft	1.0 mi	1.3 mi	1.6 mi	1.8 mi	1.9 mi	2.3 mi
Uni-8.5	6.5 dBi	4000 ft	4800 ft	1.0 mi	1.1 mi	1.4 mi	1.7 mi	1.9 mi	2.0 mi	2.4 mi
Uni-11	9 dBi	1.0 mi	1.2 mi	1.3 mi	1.4 mi	1.7 mi	2.0 mi	2.3 mi	2.5 mi	2.9 mi
Uni-13	11 dBi	1.2 mi	1.5 mi	1.6 mi	1.7 mi	2.0 mi	2.2 mi	2.6 mi	2.8 mi	3.2 mi
Uni-16	14 dBi	1.4 mi	1.7 mi	1.8 mi	1.9 mi	2.3 mi	2.6 mi	3.1 mi	3.4 mi	3.7 mi
Uni-18	15 dBi	1.5 mi	1.8 mi	1.9 mi	2.0 mi	2.5 mi	2.8 mi	3.4 mi	3.5 mi	4.0 mi
Uni-24	19 dBi	1.9 mi	2.2 mi	2.3 mi	2.4 mi	2.9 mi	3.2 mi	3.7 mi	4.0 mi	6.0 mi

**Table 6-3: BreezeNET USA/FCC Range Table - 2Mbps**

Ant. type		Omni-2	Omni-6	Omni-7	Uni-8.5	Uni-11	Uni-13	Uni-16	Uni-18	Uni-24
	Asmb gain	2 dBi	5 dBi	6 dBi	6.5 dBi	9 dBi	11 dBi	14 dBi	15 dBi	19 dBi
Omni-2	2 dBi	1500 ft	2000 ft	2300 ft	2500 ft	0.6 mi	0.7 mi	0.8 mi	0.9 mi	1.1 mi
Omni-6	5 dBi	2000 ft	2400 ft	2600 ft	2800 ft	0.7 mi	0.9 mi	1.0 mi	1.1 mi	1.3 mi
Omni-7	6 dBi	2300 ft	2600 ft	2900 ft	3000 ft	0.8 mi	1.0 mi	1.2 mi	1.3 mi	1.4 mi
Uni-8.5	6.5 dBi	2500 ft	2800 ft	3000 ft	0.6 mi	0.8 mi	1.0 mi	1.3 mi	1.3 mi	1.5 mi
Uni-11	9 dBi	0.6 mi	0.7 mi	0.8 mi	0.8 mi	0.9 mi	1.1 mi	1.4 mi	1.5 mi	1.7 mi
Uni-13	11 dBi	0.7 mi	0.9 mi	1.0 mi	1.0 mi	1.1 mi	1.2 mi	1.5 mi	1.7 mi	2.0 mi
Uni-16	14 dBi	0.8 mi	1.0 mi	1.2 mi	1.3 mi	1.4 mi	1.5 mi	1.8 mi	2.0 mi	2.6 mi
Uni-18	15 dBi	0.9 mi	1.1 mi	1.3 mi	1.3 mi	1.5 mi	1.7 mi	2.0 mi	2.2 mi	2.8 mi
Uni-24	19 dBi	1.1 mi	1.3 mi	1.4 mi	1.5 mi	1.7 mi	2.0 mi	2.6 mi	2.8 mi	3.5 mi

**Table 6-4: BreezeNET USA/FCC Range Table - 3Mbps**

Ant. type		Omni-2	Omni-6	Omni-7	Uni-8.5	Uni-11	Uni-13	Uni-16	Uni-18	Uni-24
	Asmb gain	2 dBi	5 dBi	6 dBi	6.5 dBi	9 dBi	11 dBi	14 dBi	15 dBi	19 dBi
Omni-2	2 dBi	500 ft	750 ft	800 ft	850 ft	1200 ft	1600 ft	0.4 mi	0.5 mi	0.6 mi
Omni-6	5 dBi	750 ft	900 ft	1000 ft	1100 ft	1600 ft	2000 ft	0.5 mi	0.6 mi	0.7 mi
Omni-7	6 dBi	800 ft	1000 ft	1000 ft	1200 ft	1700 ft	2100 ft	0.6 mi	0.7 mi	0.8 mi
Uni-8.5	6.5 dBi	850 ft	1100 ft	1200 ft	1400 ft	2200 ft	0.5 mi	0.7 mi	0.7 mi	0.9 mi
Uni-11	9 dBi	1200 ft	1600 ft	1700 ft	2200 ft	0.5 mi	0.6 mi	0.8 mi	0.9 mi	1.0 mi
Uni-13	11 dBi	1600 ft	2000 ft	2100 ft	0.5 mi	0.6 mi	0.7 mi	0.9 mi	1.0 mi	1.2 mi
Uni-16	14 dBi	0.4 mi	0.5 mi	0.6 mi	0.7 mi	0.8 mi	0.9 mi	1 mi	1.1 mi	1.4 mi
Uni-18	15 dBi	0.5 mi	0.6 mi	0.7 mi	0.7 mi	0.9 mi	1.0 mi	1.1 mi	1.2 mi	1.5 mi
Uni-24	19 dBi	0.6 mi	0.7 mi	0.8 mi	0.9 mi	1.0 mi	1.2 mi	1.4 mi	1.5 mi	2 mi

**NOTE:**

The use of an LNA can improve the range by 30%-40%. To achieve this it is necessary to install an LNA on both sides of the link (in each site). An LNA will NOT enlarge the link if it is installed only on one side of the link. When using an LNA you must use two antennas - one for TX and one for RX.

## ETSI Outdoor Range Tables (Europe and Rest-of-World) – D Models, DL Models

In order to comply with ETSI regulations, 20dBm (100mW) EIRP units using antenna kits indicated as low must be configured to the low power setting (10dBm).

Using BreezeNET PRO.11 DL model with an 18dbi antenna and lowering the output power of the unit complies with ETSI regulations and improves reception. Installing this antenna at both ends of the link increases the total range. Installing this antenna at one end of the link does not increase the range, but it does increase the throughput of traffic received at the end with the 18 dBi antenna.

The following tables are compliant with ETSI regulations.

**Table 6-5: BreezeNET Europe and ROW Range Table – D Models, DL Models**  
**Data Rate = 1Mbps, Sen=-81dBm**

Antenna Kit	Omni-2	Omni-6	Uni-8.5	Uni-18/20 (DL model)	Uni-18/15 (DL model)	Uni-18/10 (DL model)
Omni-2	710m	790m	750m	670m	730m	790m
Omni-6	790m	890m	840m	750m	820m	890m
Uni-8.5	750m	840m	790m	710m	770m	840m
Uni-18/20 (low)	670m	750m	710m	1,910m	2,020m	2,130m
Uni-18/15 (low)	730m	820m	770m	2,020m	2,130m	2,250m
Uni-18/10 (low)	790m	890m	840m	2,130m	2,250m	2,370m

**Table 6-6: BreezeNET Europe and ROW Range Table – D Models****Data Rate = 2Mbps, Sen=-75dBm**

Antenna Kit	Omni-2	Omni-6	Uni-8.5	Uni-18/20 (DL model)	Uni-18/15 (DL model)	Uni-18/10 (DL model)
Omni-2	350m	400m	380m	330m	370m	400m
Omni-6	400m	450m	420m	380m	410m	450m
Uni-8.5	380m	420m	400m	350m	390m	420m
Uni-18/20 (low)	330m	380m	350m	1,240m	1,310m	1,380m
Uni-18/15 (low)	370m	410m	390m	1,310m	1,380m	1,460m
Uni-18/10 (low)	400m	450m	420m	1,380m	1,460m	1,540m

**Table 6-7: BreezeNET Europe and ROW Range Table – D Models, DL Models****Data Rate = 3Mbps, Sen=-67dBm**

Antenna Kit	Omni-2	Omni-6	Uni-8.5	Uni-18/20 (DL models)	Uni-18/15 (DL models)	Uni-18/10 (DL models)
Omni-2	140m	160m	150m	130m	150m	160m
Omni-6	160m	180m	170m	150m	160m	180m
Uni-8.5	150m	170m	160m	140m	150m	170m
Uni-18/20 (low)	130m	150m	140m	560m	610m	670m
Uni-18/15 (low)	150m	160m	150m	610m	670m	730m
Uni-18/10 (low)	160m	180m	170m	670m	730m	790m

**NOTE:**

All antennas above 8.5 (i.e. 12, 18, and 24), require a filter to be ETSI-compliant.

## ETSI Outdoor Range Tables (Europe and Rest-of-World) – DE Models

The following tables are compliant with ETSI regulations.

**Table 6-8: BreezeNET Europe and ROW Range Table – DE Models**

**Data Rate = 1Mbps, Sen=-85dBm**

Antenna Kit	Uni-24/20	Uni-24/15	Uni-24/10
Uni-24/20	3,920m	4,140m	4,370m
Uni-24/15	4,140m	4,370m	4,610m
Uni-24/10	4,370m	4,610m	4,870m

**Table 6-9: BreezeNET Europe and ROW Range Table – DE Models**

**Data Rate = 2Mbps, Sen=-79dBm**

Antenna Kit	Uni-24/20	Uni-24/15	Uni-24/10
Uni-24/20	2,550m	2,690m	2,840m
Uni-24/15	2,690m	2,840m	3,000m
Uni-24/10	2,840m	3,000m	3,160m

**Table 6-10: BreezeNET Europe and ROW Range Table – DE Models**

**Data Rate = 3Mbps, Sen=-71dBm**

Antenna Kit	Uni-24/20	Uni-24/15	Uni-24/10
Uni-24/20	1,430m	1,510m	1,600m
Uni-24/15	1,510m	1,600m	1,680m
Uni-24/10	1,600m	1,680m	1,780m

### NOTES:

All antennas above 8.5 (i.e. 12, 18, and 24), require a filter to be ETSI-compliant. The use of an LNA can improve the range by 30%-40%. To achieve this it is necessary to install an LNA on both sides of the link (in each site). An LNA will NOT enlarge the link if it is installed only on one side of the link. When using an LNA you must use two antennas - one for TX and one for RX.

## Non-Regulated Outdoor Range Tables – D Models

The following tables refer to unregulated ranges.

**Table 6-11: BreezeNET Non-Regulation Range Table – D Models**

**Data Rate = 1Mbps, Sen=-81dBm**

Antenna Kits	Omni-2	Omni-6	Uni-8.5	Uni-18/20	Uni-18/15	Uni-18/10	Uni-24/20	Uni-24/15	Uni-24/10
Omni-2	710m	790m	750m	1,980m	2,090m	2,210m	3,050m	3,220m	3,400m
Omni-6	790m	890m	840m	2,130m	2,250m	2,370m	3,280m	3,460m	3,650m
Uni-8.5	750m	840m	790m	2,050m	2,170m	2,290m	3,160m	3,340m	3,520m
Uni-18/20	1,980m	2,130m	2,050m	4,870m	5,140m	5,420m	7,500m	7,910m	8,350m
Uni-18/15	2,090m	2,250m	2,170m	5,140m	5,420m	5,730m	7,910m	8,350m	8,820m
Uni-18/10	2,210m	2,370m	2,290m	5,420m	5,730m	6,040m	8,350m	8,820m	9,310m
Uni-24/20	3,050m	3,280m	3,160m	7,500m	7,910m	8,350m	11,550m	12,190m	12,860m
Uni-24/15	3,220m	3,460m	3,340m	7,910m	8,350m	8,820m	12,190m	12,860m	13,580m
Uni-24/10	3,400m	3,650m	3,520m	8,350m	8,820m	9,310m	12,860m	13,580m	14,330m

**Table 6-12: BreezeNET Non-Regulation Range Table – D Models**

**Data Rate = 2Mbps, Sen=-75dBm**

Antenna Kits	Omni-2	Omni-6	Uni-8.5	Uni-18/20	Uni-18/15	Uni-18/10	Uni-24/20	Uni-24/15	Uni-24/10
Omni-2	350m	400m	380m	1,290m	1,360m	1,430m	1,980m	2,090m	2,210m
Omni-6	400m	450m	420m	1,380m	1,460m	1,540m	2,130m	2,250m	2,370m
Uni-8.5	380m	420m	400m	1,330m	1,410m	1,490m	2,050m	2,170m	2,290m
Uni-18/20	1,290m	1,380m	1,330m	3,160m	3,340m	3,520m	4,870m	5,140m	5,420m
Uni-18/15	1,360m	1,460m	1,410m	3,340m	3,520m	3,720m	5,140m	5,420m	5,730m
Uni-18/10	1,430m	1,540m	1,490m	3,520m	3,720m	3,920m	5,420m	5,730m	6,040m
Uni-24/20	1,980m	2,130m	2,050m	4,870m	5,140m	5,420m	7,500m	7,910m	8,350m
Uni-24/15	2,090m	2,250m	2,170m	5,140m	5,420m	5,730m	7,910m	8,350m	8,820m
Uni-24/10	2,210m	2,370m	2,290m	5,420m	5,730m	6,040m	8,350m	8,820m	9,310m

**Table 6-13: BreezeNET Non-Regulation Range Table – D Models**  
**Data Rate = 3Mbps, Sen=-67dBm**

Antenna Kits	Omni-2	Omni-6	Uni-8.5	Uni-18/20	Uni-18/15	Uni-18/10	Uni-24/20	Uni-24/15	Uni-24/10
Omni-2	140m	160m	150m	600m	650m	710m	1,110m	1,180m	1,240m
Omni-6	160m	180m	170m	670m	730m	790m	1,200m	1,260m	1,330m
Uni-8.5	150m	170m	160m	630m	690m	750m	1,150m	1,220m	1,290m
Uni-18/20	600m	670m	630m	1,780m	1,880m	1,980m	2,740m	2,890m	3,050m
Uni-18/15	650m	730m	690m	1,880m	1,980m	2,090m	2,890m	3,050m	3,220m
Uni-18/10	710m	790m	750m	1,980m	2,090m	2,210m	3,050m	3,220m	3,400m
Uni-24/20	1,110m	1,200m	1,150m	2,740m	2,890m	3,050m	4,220m	4,450m	4,700m
Uni-24/15	1,180m	1,260m	1,220m	2,890m	3,050m	3,220m	4,450m	4,700m	4,960m
Uni-24/10	1,240m	1,330m	1,290m	3,050m	3,220m	3,400m	4,700m	4,960m	5,230m

## Extending Range using the TPA-24 and LNA-10

The following tables show examples of how outdoor ranges of D-model units can be extended using the TPA-24 and LNA-10 devices.

In the range tables below, the note LNA means that the LNA 10 Low Noise Receive Amplifier is used (see *LNA 10 Low Noise Receive Amplifier*, on page 7-4). The note TPA means that the TPA 24 Transmit Power Amplifier is used (see *TPA 24 Transmit Power Amplifier (Booster)*, on page 7-2). When the LNA or TPA are used, one of the unit's antennas should be permanently set to transmit and the other to receive. In this case, Antenna Diversity is not applicable. The use of an LNA or a Booster (TPA 24) will only enlarge the range if they are installed on both sides of the link.

The identification of "TX kit" and "RX kit" is for reference purposes only. They do not have any other meaning than for arranging the table to show the effects of the LNA and Booster (TPA 24).

For ranges over 30 km, it is recommended to consult Alvarion Technical Support or your local dealer.

**NOTE:**

In the following tables, "Omni-6/10" refers to an Omni 6dbi antenna with a 10 Meter Heliax cable.



**Table 6-14: TPA-24 and LNA-10 Extension Range Table. Data Rate = 1Mbps, Sen=81dBm**

<div> <div>Transmit and Receive Antenna Kits for Side A</div> <div>Transmit and Receive Antenna Kits for Side B</div> </div>				TX kit	Omni-6/10	Omni-6/10	Omni-6 (TPA)	Omni-6 (TPA)	Uni-18/10	Uni-18/10	Uni-18/10 (TPA)	Uni-18/10 (TPA)	Uni-24/10	Uni-24/10	Uni-24/10 (TPA)	Uni-24/10 (TPA)
				TX EIRP	21	21	30	30	33	33	42	42	39	39	48	48
				RX kit	Omni-6/10	Omni-6 (LNA 10)	Omni-6/10	Omni-6 (LNA)	Uni-18/10	Uni-18/10 (LNA)	Uni-18/10	Uni-18/10 (LNA)	Uni-24/10	Uni-24/10 (LNA)	Uni-24/10	Uni-24/10 (LNA)
				RX Gain	4	8.35	4	8.35	16	20.35	16	20.35	22	26.35	22	26.35
TX kit	EIRP	RX kit	RX Gain													
Omni-6/10	21	Omni-6/10	4		1,070m	1,070m	1,070m	1,470m	2,550m	2,550m	2,550m	3,480m	3,920m	3,920m	3,920m	5,370m
Omni-6/10	21	Omni-6 (LNA)	8.35		1,070m	1,470m	1,070m	1,470m	2,550m	3,480m	2,550m	3,480m	3,920m	5,370m	3,920m	5,370m
Omni-6 (TPA)	30	Omni-6/10	4		1,070m	1,070m	2,050m	2,050m	2,550m	2,550m	4,870m	4,870m	3,920m	3,920m	7,500m	7,500m
Omni-6 (TPA)	30	Omni-6 (LNA)	8.35		1,470m	1,470m	2,050m	2,810m	3,480m	3,480m	4,870m	6,660m	5,370m	5,370m	7,500m	10,260m
Uni-18/10	33	Uni-18/10	16		2,550m	2,550m	2,550m	3,480m	6,040m	6,040m	6,040m	8,260m	9,310m	9,310m	9,310m	12,730m
Uni-18/10	33	Uni-18/10 (LNA)	20.35		2,550m	3,480m	2,550m	3,480m	6,040m	8,260m	6,040m	8,260m	9,310m	12,730m	9,310m	12,730m
Uni-18/10 (TPA)	42	Uni-18/10	16		2,550m	2,550m	4,870m	4,870m	6,040m	6,040m	11,550m	11,550m	9,310m	9,310m	17,780m	17,780m
Uni-18/10 (TPA)	42	Uni-18/10 (LNA)	20.35		3,480m	3,480m	4,870m	6,660m	8,260m	8,260m	11,550m	15,790m	12,730m	12,730m	17,780m	24,320m
Uni-24/10	39	Uni-24/10	22		3,920m	3,920m	3,920m	5,370m	9,310m	9,310m	9,310m	12,730m	14,330m	14,330m	14,330m	19,600m
Uni-24/10	39	Uni-24/10 (LNA)	26.35		3,920m	5,370m	3,920m	5,370m	9,310m	12,730m	9,310m	12,730m	14,330m	19,600m	14,330m	19,600m
Uni-24/10 (TPA)	48	Uni-24/10	22		3,920m	3,920m	7,500m	7,500m	9,310m	9,310m	17,780m	17,780m	14,330m	14,330m	27,380m	27,380m
Uni-24/10 (TPA)	48	Uni-24/10 (LNA)	26.35		5,370m	5,370m	7,500m	10,260	12,730m	12,730m	17,780m	24,320m	19,600m	19,600m	27,380m	37,450m

**Table 6-15: TPA-24 and LNA-10 Extension Range Table. Data Rate = 2Mbps, Sen=-75dBm**

<div> <div>Transmit and Receive Antenna Kits for Side A</div> <div>Transmit and Receive Antenna Kits for Side B</div> </div>			TX kit	Omni-6/10	Omni-6/10	Omni-6 (TPA)	Omni-6 (TPA)	Uni-18/10	Uni-18/10	Uni-18/10 (TPA)	Uni-18/10 (TPA)	Uni-24/10	Uni-24/10 (TPA)	Uni-24/10 (TPA)
			TX EIRP	21	21	30	30	33	33	42	42	39	39	48
			RX kit	Omni-6/10	Omni-6 (LNA 10)	Omni-6/10	Omni-6 (LNA)	Uni-18/10	Uni-18/10 (LNA)	Uni-18/10 (LNA)	Uni-18/10 (LNA)	Uni-24/10 (LNA)	Uni-24/10 (LNA)	Uni-24/10 (LNA)
			RX Gain	4	8.35	4	8.35	16	20.35	16	20.35	22	26.35	26.35
TX kit	EIRP	RX kit	RX Gain											
Omni-6/10	21	Omni-6/10	4	560m	560m	560m	930m	1,650m	1,650m	1,650m	2,260m	2,550m	2,550m	3,480m
Omni-6/10	21	Omni-6 (LNA)	8.35	560m	930m	560m	930m	1,650m	2,260m	1,650m	2,260m	2,550m	3,480m	3,480m
Omni-6 (TPA)	30	Omni-6/10	4	560m	560m	1,330m	1,330m	1,650m	1,650m	3,160m	3,160m	2,550m	2,550m	4,870m
Omni-6 (TPA)	30	Omni-6 (LNA)	8.35	930m	930m	1,330m	1,820m	2,260m	2,260m	3,160m	4,320m	3,480m	3,480m	6,660m
Uni-18/10	33	Uni-18/10	16	1,650m	1,650m	1,650m	2,260m	3,920m	3,920m	3,920m	5,370m	6,040m	6,040m	8,260m
Uni-18/10	33	Uni-18/10 (LNA)	20.35	1,650m	2,260m	1,650m	2,260m	3,920m	5,370m	3,920m	5,370m	6,040m	8,260m	8,260m
Uni-18/10 (TPA)	42	Uni-18/10	16	1,650m	1,650m	3,160m	3,160m	3,920m	3,920m	7,500m	7,500m	6,040m	6,040m	11,550m
Uni-18/10 (TPA)	42	Uni-18/10 (LNA)	20.35	2,260m	2,260m	3,160m	4,320m	5,370m	5,370m	7,500m	10,260m	8,260m	8,260m	15,790m
Uni-24/10	39	Uni-24/10	22	2,550m	2,550m	2,550m	3,480m	6,040m	6,040m	6,040m	8,260m	9,310m	9,310m	12,730m
Uni-24/10	39	Uni-24/10 (LNA)	26.35	2,550m	3,480m	2,550m	3,480m	6,040m	8,260m	6,040m	8,260m	9,310m	12,730m	12,730m
Uni-24/10 (TPA)	48	Uni-24/10	22	2,550m	2,550m	4,870m	4,870m	6,040m	6,040m	11,550m	11,550m	9,310m	9,310m	17,780m
Uni-24/10 (TPA)	48	Uni-24/10 (LNA)	26.35	3,480m	3,480m	4,870m	6,660m	8,260m	8,260m	11,550m	15,790m	12,730m	12,730m	24,320m

**Table 6-16: TPA-24 and LNA-10 Extension Range Table. Data Rate = 3Mbps, Sen=-67dBm**

<div> <div>Transmit and Receive Antenna Kits for Side A</div> <div>Transmit and Receive Antenna Kits for Side B</div> </div>				Tx kit	Omni-6/10	Omni-6/10	Omni-6 (TPA)	Omni-6 (TPA)	Uni-18/10	Uni-18/10	Uni-18/10 (TPA)	Uni-18/10 (TPA)	Uni-24/10	Uni-24/10	Uni-24/10 (TPA)	Uni-24/10 (TPA)
				TX EIRP	21	21	30	30	33	33	42	42	39	39	48	48
				RX kit	Omni-6/10	Omni-6 (LNA 10)	Omni-6/10	Omni-6 (LNA)	Uni-18/10	Uni-18/10 (LNA)	Uni-18/10	Uni-18/10 (LNA)	Uni-24/10	Uni-24/10 (LNA)	Uni-24/10	Uni-24/10 (LNA)
				RX Gain	4	8.35	4	8.35	16	20.35	16	20.35	22	26.35	22	26.35
TX kit	EIRP	RX kit	RX Gain													
Omni-6/10	21	Omni-6/10	4		220m	220m	220m	370m	890m	890m	890m	1,270m	1,430m	1,430m	1,430m	1,960m
Omni-6/10	21	Omni-6 (LNA)	8.35		220m	370m	220m	370m	890m	1,270m	890m	1,270m	1,430m	1,960m	1,430m	1,960m
Omni-6 (TPA)	30	Omni-6/10	4		220m	220m	630m	630m	890m	890m	1,780m	1,780m	1,430m	1,430m	2,740m	2,740m
Omni-6 (TPA)	30	Omni-6 (LNA)	8.35		370m	370m	630m	1,030m	1,270m	1,270m	1,780m	2,430m	1,960m	1,960m	2,740m	3,740m
Uni-18/10	33	Uni-18/10	16		890m	890m	890m	1,270m	2,210m	2,210m	2,210m	3,020m	3,400m	3,400m	3,400m	4,650m
Uni-18/10	33	Uni-18/10 (LNA)	20.35		890m	1,270m	890m	1,270m	2,210m	3,020m	2,210m	3,020m	3,400m	4,650m	3,400m	4,650m
Uni-18/10 (TPA)	42	Uni-18/10	16		890m	890m	1,780m	1,780m	2,210m	2,210m	4,220m	4,220m	3,400m	3,400m	6,490m	6,490m
Uni-18/10 (TPA)	42	Uni-18/10 (LNA)	20.35		1,270m	1,270m	1,780m	2,430m	3,020m	3,020m	4,220m	5,770m	4,650m	4,650m	6,490m	8,880m
Uni-24/10	39	Uni-24/10	22		1,430m	1,430m	1,430m	1,960m	3,400m	3,400m	3,400m	4,650m	5,230m	5,230m	5,230m	7,160m
Uni-24/10	39	Uni-24/10 (LNA)	26.35		1,430m	1,960m	1,430m	1,960m	3,400m	4,650m	3,400m	4,650m	5,230m	7,160m	5,230m	7,160m
Uni-24/10 (TPA)	48	Uni-24/10	22		1,430m	1,430m	2,740m	2,740m	3,400m	3,400m	6,490m	6,490m	5,230m	5,230m	10,000m	10,000m
Uni-24/10 (TPA)	48	Uni-24/10 (LNA)	26.35		1,960m	1,960m	2,740m	3,740m	4,650m	4,650m	6,490m	8,880m	7,160m	7,160m	10,000m	13,680m

# Available Antennas and Antenna Kits

This following table describes several transmit/receive antennas that function well with BreezeNET PRO.11 units.

**Table 6-17: FCC Available Antennas (USA)**

Model	Ant. Gain	Cable Len	Kit Contains:	Ideal for:	Dispersion	Dimensions H x W x D
OMNI-2	2 dBi	N/A	2 OMNI-2 Antennas Proprietary SMA	Converting "D" Models for use indoors	360°H/ 60° V	3"x.5" Tubular
OMNI-6	6 dBi	4-ft	OMNI-6 Antenna Mounting Hardware 4-ft Cable Assembly	Extending indoor range of access points and station adapters	360°H/ 26° V	13"x0.75" Tubular
OMNI-7.2	7.2 dBi	20-ft	OMNI-7.2 Antenna Mounting Hardware 20-ft Cable Assembly	Establishing 360° coverage for outdoor multipoint links	360°H/ 22° V	16"x0.75" Tubular
UNI-8.5	8.5 dBi	8-ft	UNI-8.5 Antenna Mounting Hardware 8-ft Cable	Extending indoor range of access points and/or station adapters	75°H/ 60° V	4"x3.7"x1.2"
UNI-8.5Ext	8.5 dBi	8-ft	UNI-8.5 Antenna Mounting Hardware 8-ft Cable Assembly	Short range outdoor multipoint links	75°H/ 60° V	4"x3.7"x1.2"
UNI-11P-75	11 dBi	30-ft	UNI-11P-75 Antenna Mounting Hardware 30-ft Cable Assembly	ISPs, school districts, and campus area networks requiring wide dispersion patterns	75°H/ 28° V	11"x7.5"x3.5"

Model	Ant. Gain	Cable Len	Kit Contains:	Ideal for:	Dispersion	Dimensions H x W x D
UNI-13P	13 dBi	20-ft	UNI-13P Antenna Mounting Hardware 20-ft Cable Assembly	Medium range outdoor multipoint links	46°H/ 28° V	11"x7.5"x3.5"
UNI-16P	16 dBi	30-ft	UNI-16P Antenna Mounting Hardware 30-ft Cable Assembly	Medium to long range outdoor multipoint links requiring compact form factors	28°H/ 28° V	11"x11"x3.5"
UNI-18	18 dBi	30-ft	UNI-18 Antenna Mounting Hardware 30-ft Cable Assembly	Long range outdoor point-to-point and multipoint links	12°H/ 14° V	16"x20"x15"
UNI-24	24 dBi	50-ft	UNI-24 Antenna Mounting Hardware 50-ft Cable Assembly	Long range outdoor point-to-point links	6°H/ 10° V	24"x36"x15"

**Table 6-18: ETSI Available Antennas (Europe and Rest-of-World)**

<b>Model</b>	<b>Ant. Gain</b>	<b>Cable Len</b>	<b>Kit Contains:</b>	<b>Ideal for:</b>	<b>Dispersion</b>	<b>Dimensions H x W x D</b>
OMNI-2	2 dBi	N/A	2 OMNI-2 Antennas Proprietary SMA	Converting "D" Models for use indoors	360°H/ 60° V	3"x.5" Tubular
OMNI-6	6 dBi	3m	OMNI-6 Antenna 90° Mount Bracket 3m RG-58 Cable	Extending indoor range of access points and station adapters	360°H/ 26° V	13"x0.75" Tubular
UNI-8.5	8.5 dBi	6m	UNI-8.5 Antenna Wall Mounting HW 6m RG-58 Cable	Extending indoor range of access points and/or station adapters	75°H/ 60° V	4"x3.7"x1.2"
UNI-18/10 UNI-18/15 UNI-18/20	18 dBi	10m 15m 20m	UNI-18 Antenna U-bolt for pole Helix Cable	Long range outdoor point-to-point and multipoint links	12°H/ 14° V	16"x20"x15"
UNI-24/10 UNI-24/15 UNI-24 /20	24 dBi	10m 15m 20m	UNI-24 Antenna U-bolt for pole Helix Cable	Long range outdoor point-to-point links	6°H/ 10° V	24"x36"x15"

# Precautions

Detached antennas, whether installed indoors or out, should be installed **ONLY** by experienced antenna installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities.

Failure to do so may void the BreezeNET Product Warranty and may expose the end user to legal and financial liabilities. Alvarion and its resellers or distributors are not liable for injury, damage or violation of government regulations associated with the installation of detached antennas.

## Transmit Antenna

Regulations regarding maximum antenna gains vary from country to country. It is the responsibility of the end user to operate within the limits of these regulations and to ensure that the professional installer is aware of these regulations, as well. The FCC in the United States and ETSI in Europe limit effective transmit power to 36dBm (USA) and 20dBm (Europe). The maximum total assembly gain of antennas and cables in this case equals 19dBi (USA) and 3dBi (Europe).

Violation of government regulations exposes the end user to legal and financial liabilities. Alvarion and its resellers and distributors shall not be liable for expense or damage incurred as a result of installations which exceed local transmit gain limitations.

## Spurious Radio Frequency Emissions

The regulations referred to in the previous section also specify maximum “out-of-band” radio frequency emissions. Install a filter as close as possible to the BreezeNET PRO.11 “D” model unit connector.

## Lightning Protection

Lightning protection is designed to protect people, property and equipment by providing a path to ground for the lightning's energy. The lightning arrestor diverts the strike energy to ground through a deliberate and controlled path instead of allowing it to choose a random path. Lightning protection for a building is more forgiving than protection of electronic devices. A building can withstand up to 100,000 volts, but electronic equipment may be damaged by just a few volts.

Lightning protection entails connecting an antenna discharge unit (also called an arrestor) to each cable as close as possible to the point where it enters the building. It also entails proper grounding of the arrestors and of the antenna mast (if the antenna is connected to one).

The lightning arrestor should be installed and grounded at the point where the cable enters the building. The arrestor is connected to the unit at one end and to the antenna at the other end.

The professional installer you choose must be knowledgeable about lightning protection. The installer must install the lightning protector in a way that maximizes lightning protection. Alvarion offers the following high-quality lightning arrestor assembly:

BreezeNET AL 1 Lightning Arrestor - Part No. 872905 5 ft (1.5m), "N" Male to "N" Female.

## Rain Proofing

12, 18, and 24 dBi antennas must be sealed against rain at the point the cable enters the pole before they are suitable for external use.





# Chapter 7

## Accessory Installation

### About This Chapter

This chapter introduces some of the accessories available for specific installations, and describes how to install them.

This chapter is comprised of the following sections:

- ♦ **TPA 24 Transmit Power Amplifier (Booster)**, page 7-2, describes the functionality and how to install the power amplifier.
- ♦ **LNA 10 Low Noise Receive Amplifier**, page 7-4, describes the functionality and how to install the low noise receive amplifier.
- ♦ **RFS 122 Radio Frequency Splitter**, page 7-7, describes the operation and how to install the radio frequency splitter.
- ♦ **AL 1 Lightning Arrestor**, page 7-8, describes how to protect people and equipment from the danger of electrical shock due to lightning.
- ♦ **AMP 2440 Bi-Directional Amplifier**, page 7-9, provides the specifications and installation procedures for the bi-directional amplifier.

## TPA 24 Transmit Power Amplifier (Booster)

The TPA 24 Transmit Power Amplifier is used to amplify the transmit power to a fixed output of 24 dBm (250 mW). The TPA 24 is especially useful when long RF cable runs are required. In addition, the TPA 24 simplifies antenna alignment by enabling the use of wider dispersion transmit antennas. The TPA 24 is internally protected against lightning and voltage surge protection.

There are two models:

- ◆ The TPA 24 NL receives input power in the range of -10dBm to 0dBm.
- ◆ The TPA 24 NH receives an input power of 0dBm to +10dBm.

Both models amplify the input power to a fixed output level of 24dBm (250mW).

The TPA is powered by 12VDC carried from the power inserter by the RF cable.

**NOTE:**

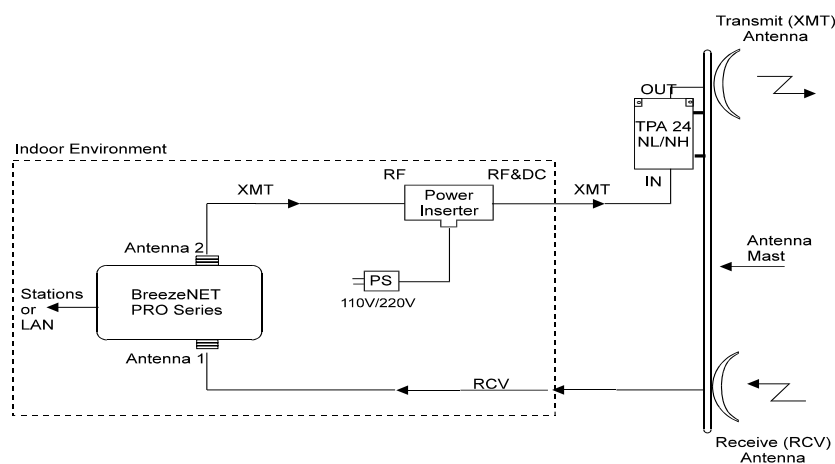
The TPA 24 is not available in the USA due to FCC regulations.

When used in compliance with ETSI regulations, the TPA 24 can be connected to cables and antennas resulting in a total transmitted power of 20dBm (100 mW) EIRP.

For technical specifications, refer to *Specifications for TPA 24 Transmit Power Amplifier*, on page A-28.

## Installing the TPA 24

1. Choose one of the TPA 24 models according to the power level at the input of the booster. In general the NH model is used. For installations with long cables (high attenuation), the NL model should be used.
2. Choose one of the antenna connectors to be used for transmission. This connector is called the transmit antenna of the unit.
3. Configure the BreezeNET PRO.11 unit via a local terminal to transmit through the transmit antenna using the **Transmit Diversity** parameter (see *Wireless LAN (WLAN) Parameters*, on page 3-16).



**Figure 7-1: TPA 24 Installation**

4. Connect the TPA 24 RF output directly to the transmit antenna.
5. Attach the TPA 24 RF input to the Power Inserter with the RF cable. The Power Inserter must be installed indoors.
6. Connect the RF cable leading from the Power Inserter to the transmit antenna on the BreezeNET PRO.11 unit.

7. Plug the power cable leading from the Power Inserter into any available 110/220V outlet. The power supply must be installed indoors.
8. For reception, use a separate antenna connected to the other antenna connector of the BreezeNET unit.

**NOTE:**

Installations exceeding regulations set by local authorities expose the installer and the user to potential legal and financial liabilities.

## LNA 10 Low Noise Receive Amplifier

The LNA 10 is a high-performance, low-noise pre-amplifier designed to enhance fringe area reception and provide additional gain on the receive antenna. Its exceptionally small size and light weight enables it to be directly mounted on the antenna by means of the female RF IN connector. Power is obtained through an RG-59 coaxial cable connected to the power supply. The LNA 10 is internally protected against lightning and voltage surge protection.

The Power Supply (PS) and Power Inserter are supplied with the LNA 10. The RG-59 coaxial cable with F-type connector is not supplied and must be purchased separately.

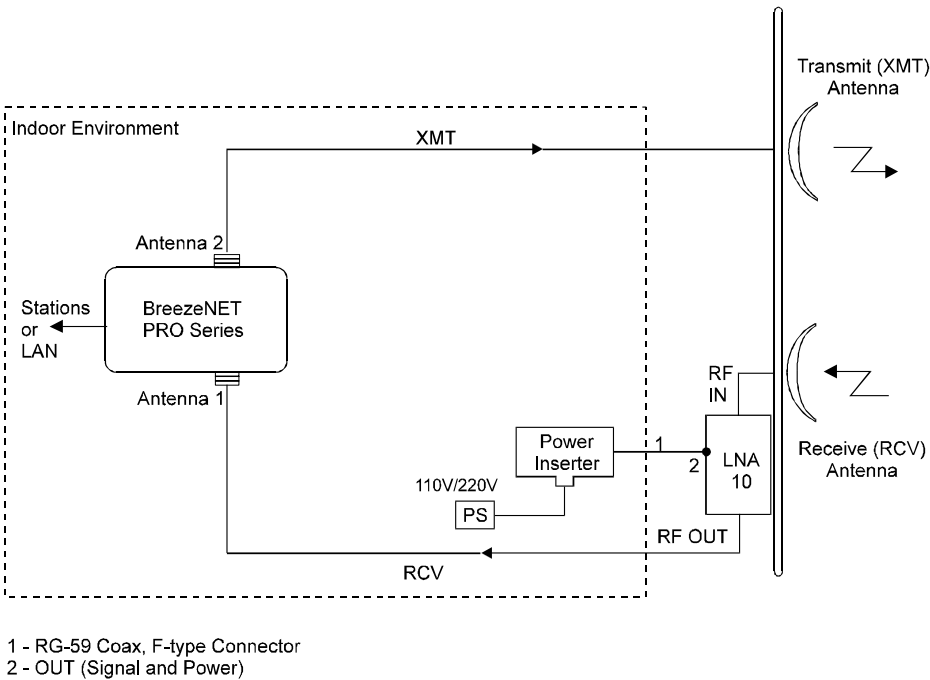
For technical specifications, refer to *Specification for LAN 10 Low Noise Receive Amplifier*, on page A-29.

## Installing the LNA 10

Before installing the LNA 10, the following steps must be taken:

- 1.** Choose one of the antenna connectors to be used for reception. This connector is called the receive antenna of the unit. The other connector is called the transmit antenna of the unit.
- 2.** Configure the BreezeNET PRO.11 unit via the Monitor to transmit through the transmit antenna only using the **Transmit Diversity** parameter (see *Wireless LAN (WLAN) Parameters*, on page 3-16). This prevents transmission from going through the LNA 10.
- 3.** Connect the LNA 10 RF input directly to the receive antenna, as close as possible.
- 4.** Attach the LNA 10 RF output directly to the RF cable going down to the receive antenna connector on the BreezeNET PRO.11 unit.
- 5.** Connect the RG-59 coaxial cable, which leads down to the Power Inserter, to the “Signal and Power out” connector on the LNA 10.
- 6.** Connect the Power Inserter to the power supply (both are indoor units).

7. For transmission, use a separate antenna connected to the other antenna connector (transmit antenna) of the BreezeNET unit.



### Figure 7-2: LNA 10 Connections Diagram

## RFS 122 Radio Frequency Splitter

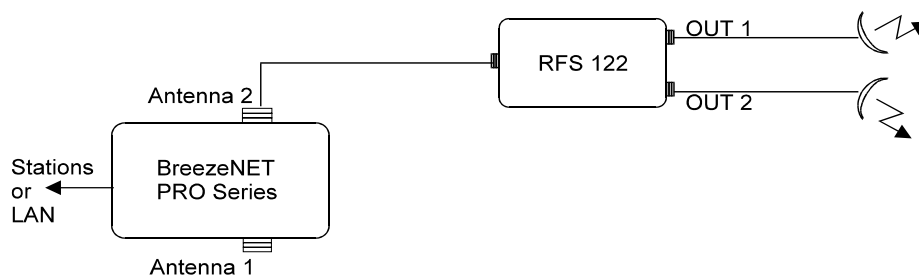
The RFS 122 Radio Frequency Splitter is used to split the RF signal generated by a transmitter into two signals. These signals are then sent to two different and independent antennas. The RFS 122 enables radio transmission using two directional antennas connected to the same port of the BreezeNET PRO.11 unit. Similarly, the splitter is used to combine two receiving antennas to one antenna connector.

Before installing the RFS 122, configure the BreezeNET PRO.11 unit via the Monitor to transmit through Antenna 2 only using the **Transmit Diversity** parameter (see *Wireless LAN (WLAN) Parameters*, on page 3-16), and connect the RFS 122 to antenna connector 2.

For technical specifications, refer to *Specifications for RFS 122 Radio Frequency Splitter*, on page A-30.

### Installing the RFS 122

The following diagram illustrates RFS-122 installation.

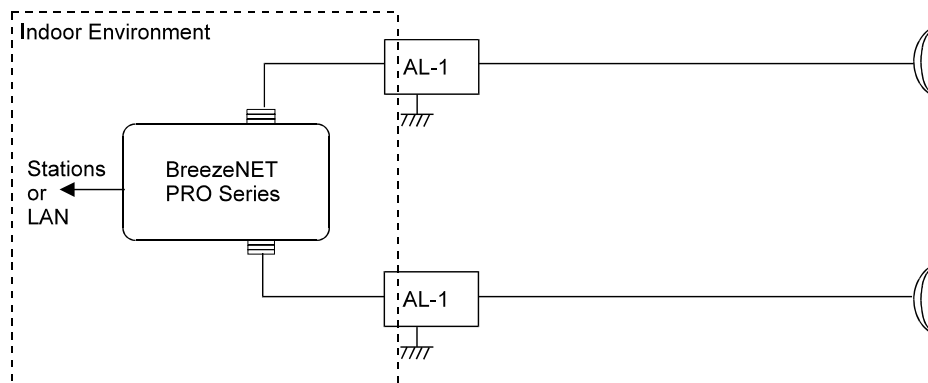


**Figure 7-3: RFS-122 Connection Diagram**

## AL 1 Lightning Arrestor

The AL 1 Lightning Arrestor is used to protect transmitters and receivers from transients originating from lightning or EMP.

The AL 1 is gas tube-based and is not radioactive. The gas discharge tube can sustain several transients if the time period between transients is sufficient to allow the tube to cool down.



**Figure 7-4: AL-1 Connection Block Diagram**

One of the female type N connectors is mounted directly through a hole in the shelter wall and held in place with a lock washer and nut.

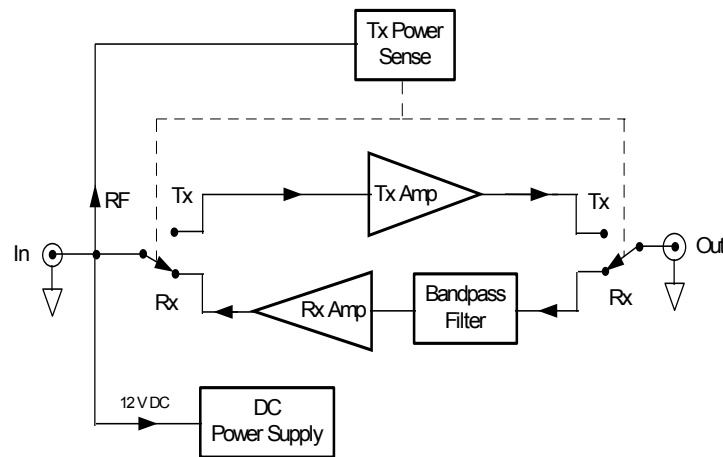


## AMP 2440 Bi-Directional Amplifier

The AMP 2440 is a bi-directional amplifier designed for extending the range of BreezeNET wireless LAN radios.

The unit operates automatically; therefore there is no need for manual adjustments. The units receive signal gain and also provide transmit power amplification.

For technical specifications, refer to *Specifications for AMP 2440 Bi-Directional Power Amplifier*, on page A-32.



**Figure 7-5: AMP 2440 Functional Block Diagram**

The amplifier is installed directly at the antenna's feed point, providing maximum effectiveness of transmit power which compensates for signal loss in the transmitter cable to the antenna. Likewise, the Low Noise Amplifier (LNA) in the AMP 2440 boosts the receive signal right at the antenna prior to experiencing the loss in the transmission cable to the radio. This gain also overcomes the losses in the transmission cable between the amplifier and the radio. In fact, use of the AMP 2440 bi-directional amplifier will actually increase the receiver sensitivity of the radio by 4dB. The ultimate result is the best possible noise figure and maximum receiver sensitivity. System gains of up to 30 dB are typical when amplifiers are used at each end of a link.

The AMP 2440 bi-directional amplifier is completely weatherproof and can be bolted to the antenna mast or tower leg using the U-bolt included. The connectors face down so that gravity will drain all water away from the amplifier enclosure. This will prevent water from settling on the face of the unit. Likewise, since the LEDs are also facing downward they can be checked for operation from the bottom of the mast.

DC Power to the amplifier is supplied through the transmission cable, using an indoor power supply and DC Injector. The amplifier unit also contains its own integral lightning protection and DC surge protection to ensure years of continuous outdoor operation.

Alvarion provides the user with two models of the AMP 2440 bi-directional amplifier:

- ◆ AMP 2440-500. Provides 500 mW (+27dBm) maximum output
- ◆ AMP 2440-250. Provides 250 mW (+24dBm) maximum output

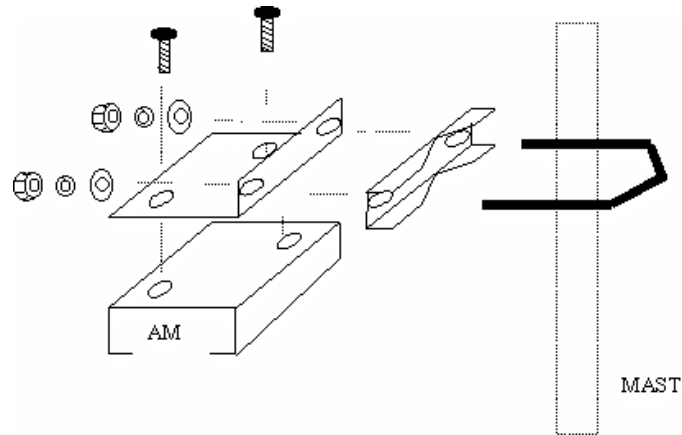
The transmit gain for **both** models is 12 - 15dB. Full output power of approximately 500 mW is achieved with 30 mW (+15 dBm) input to the amplifier; 8 mW (+9dBm) for the AMP 2440-250 model. The amplifier goes into limiting at this point and higher input power results in only slight increases in the output power. Up to 100 mW of power may be safely applied directly to the amplifier input without any damage on either model.

The AMP 2440 bi-directional amplifier comes with power supplies that have standard 2.1 mm barrel plugs (which are configured as positive (+) tip and negative (-) outer conductor). Although normally supplied with a power supply, any regulated 12 Volt DC 1 amp supply can be used. The power supply can be used with 110 or 240 VAC power.

## **Installing the AMP 2440 Bi-Directional Amplifier**

The AMP 2440 bi-directional amplifier is designated for installation by professional radio installers. Several key factors unique to the particular installation determine the power level at the input of the amplifier. The most important consideration is the cable loss in the transmission cable between the radio and the pole mounted amp. The installer should understand these and other factors when computing the input power to the amplifier.

The AMP 2440 bi-directional amplifier can be mast mounted using the steel U-bolt included with the unit. The AMP 2440 bi-directional amplifier should be installed with the connectors facing downward. After placing the assembly on the mast, use an open-end wrench to carefully tighten the nuts. Take care not to over-tighten the nuts or you may inadvertently strip the threads.



**Figure 7-6: AMP 2440 Installation and Mounting**

**WARNING:**

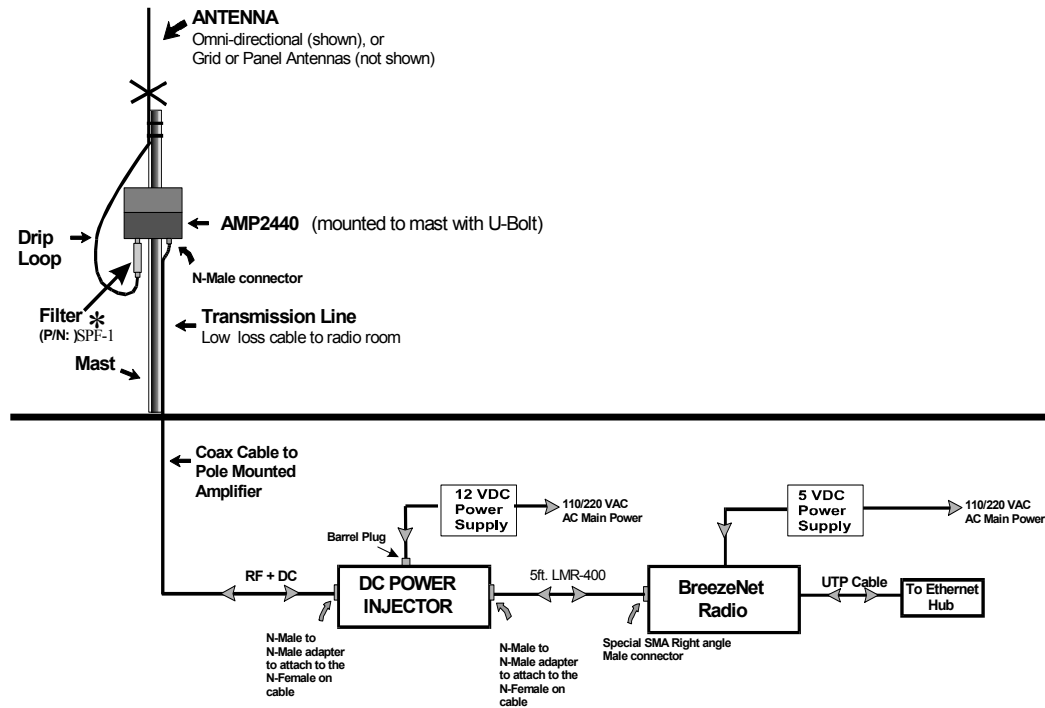
It is very important to waterproof the RF connectors on the AMP 2440 bi-directional amplifier.

However, it is recommended that you do not seal the connectors until after all system tests have been performed. Be sure to use the high quality weather resistant vapor wrap included with your amplifier kit to seal all the outside connections.

The DC Power Injector is not in a waterproof enclosure and must be protected from the weather. It can be permanently mounted to a surface using the mounting flanges.

**NOTE:**

When using the 24dB gain dish antenna in the United States, the external filter (P/N: SPF-1) must be installed to comply with FCC emission requirements.



\* Filter is required in the United States when the 24dB grid dish antenna is used in order to comply with FCC emission requirements.

For grounding, mount one of the female N-Type connectors directly through a hole in the shelter wall and fix it in place with a lock-washer and nut.





## Chapter 8

# Upgrade Procedure

Firmware upgrades to the unit's flash memory is done by a simple download procedure using a TFTP application of any kind. Before beginning an upgrade, be sure you have the correct files and latest instructions.

Upgrade packages can be obtained at the Alvarion web site:

*<http://www.alvarion.com>.*

The BreezeNET firmware includes a two-code mechanism which allows the user to revert back and forth between the currently installed versions of the unit. One version is assigned as Active code, the second version is assigned as Non-Active code.

The user can download a newer version that replaces the currently assigned Active code version. The old Active code is reassigned as the Non-Active code, and the old Non-Active code is erased from the unit.

**NOTE:**

Version 5.1.37 can only be loaded to units running version 5.X.X (new HW).

➤ **To download a new version:**

- 1.** Set up an IP connection to the device. You can verify that the connection is working using the Ping command.
- 2.** Run TFTP software of any kind and connect to the device.

3. Send the file to the unit's IP address, using the TFTP application. For the source file name, use the code file supplied by Alvarion; for the destination file name, use the SNMP write community parameter defined in the unit. The default write community parameter is **private**. For example: TFTP -i 192.122.123.12 PUT <load file name> private. The load file name is N5\_1\_37.AP for the AP10 and N5\_1\_37.SA for the SA10, SA40 and WB10 stations.
4. Do not reset the device during the download procedure. The unit resets itself and powers up with the new upgraded version.

The new version is downloaded to the unit by replacing the Active code. The old version becomes the new Non-Active code and the old Non-Active code is erased from the unit.

## Maintaining Present Device Settings after Firmware Upgrade

The new firmware version can be downloaded without losing the existing configuration settings. To retain the existing parameter configuration when upgrading:

- ◆ **For 5.0.63 and earlier releases of version 5 to 5.1.37:** The installer must export the configuration file via TFTP. The name of the configuration file is "private.cfg". The "get" TFTP action causes the configuration parameters to be saved on the FLASH memory. After the upgrade process is complete, the new version: 5.1.37 restores the saved configuration parameters from the FLASH.
- ◆ **From version 5.0.143 and higher to 5.1.37:** There is no need for any command input, the current configuration is saved automatically.



## Chapter 9

# System Troubleshooting



### About This Chapter

The following troubleshooting guide provides answers to some of the more common problems that may occur when installing and using BreezeNET PRO.11 series products. If problems not mentioned in this guide should arise, checking the Ethernet and WLAN counters may help. If the problem persists, please feel free to contact your local distributor or the Alvarion Technical Support Department.

This chapter is comprised of the following sections:

- ♦ **Troubleshooting Guide**, page 9-2, provides answers to the most common installation and initial operation challenges.
- ♦ **Checking Counters**, page 9-7, describes how to check the counters for additional performance problems that might arise.

# Troubleshooting Guide

Problem and Indication	Possible Cause	Corrective Action
No Power to Unit. PWR LED is off.	<ol style="list-style-type: none"><li>1. Power cord is not properly connected.</li><li>2. Power supply is defective.</li></ol>	<ol style="list-style-type: none"><li>1. Verify power cord is properly connected to the BreezeNET unit and to the power outlet.</li><li>2. If this is not the cause, replace the power supply.</li></ol>
Failure to establish wireless link. WLNK LED is off and unit resets every few minutes.	<ol style="list-style-type: none"><li>1. Power supply to units may be faulty</li><li>2. The units may not have the same ESSID as the AP-10.</li></ol>	<ol style="list-style-type: none"><li>1. Verify power to units (AP and SA/ WB).</li><li>2. Verify that all units in the network have the same ESSID as the AP (ESSID must be identical in all units in the network):</li><li>3. Verify wireless link:  Set AP and unit (SA or WB) side by side.  Power on each unit and see if a wireless link is established (even "D" models without their external antennas should establish a link if placed side by side with the AP).  If the units fail to associate, reset units to factory default values, reset unit. The units should now establish a wireless link.</li></ol>

Problem and Indication	Possible Cause	Corrective Action
Failure to establish wireless link (D models/external antennas)	<ol style="list-style-type: none"><li>1. Power supply to units may be faulty.</li><li>2. Cables may be improperly connected</li><li>3. There may be some problem with antenna installation.</li></ol>	<ol style="list-style-type: none"><li>1. Verify power to units.</li><li>2. Verify that all cables are connected securely.</li><li>3. Refer to previous Section and verify wireless link between the units.</li><li>4. Verify that the antenna(s) are properly installed (see relevant Section in this manual):  Check antenna alignment.  Verify that antenna polarization is the same at both ends.  Verify that the range matches specifications.  Verify line-of-sight/antenna alignment/antenna height.</li></ol>
Wireless link established, but there is no Ethernet activity (AP and WB units).	<ol style="list-style-type: none"><li>1. Ethernet hub port or UTP cable is faulty.</li><li>2. Ethernet port in unit is faulty.</li></ol>	<ol style="list-style-type: none"><li>1. Check that the LINK LED is on and solid at the hub port. If this is not the case, the port is inactive. Try another port on the hub or another UTP cable.</li><li>2. Verify that Ethernet port in unit is working. Ping unit to verify Ethernet connection.</li><li>3. Verify that you are using a cross-over UTP cable (pins 1 &amp; 3, 2 &amp; 6) if connected directly to workstation, or a straight-through cable if connected to a hub.</li><li>4. Check ETHR LED indicator in unit and Ethernet counters in Monitor to verify Ethernet activity.</li></ol>

Problem and Indication	Possible Cause	Corrective Action
Wireless link established, but there is no Ethernet activity (SA-10 and SA-40 units).	<ol style="list-style-type: none"> <li>1. Ethernet port on Network Interface card is faulty.</li> <li>2. Ethernet port of unit is faulty.</li> <li>3. UTP cable is faulty.</li> </ol>	<ol style="list-style-type: none"> <li>1. Verify that the LINK LED is lit and solid at the NIC port. If this is not the case, the port is inactive. Try using another UTP cable or another workstation.</li> <li>2. Ping the unit to check the Ethernet port. If you cannot ping the unit, this may indicate failure of cable, Ethernet port of unit or Ethernet port of workstation's NIC. Change UTP cable and retry. If you still cannot ping the unit, exchange units and try to ping the new unit using the same NIC and cable.</li> </ol>
No network detected at Station Adapter (SA-10, SA-40) workstation.	<ol style="list-style-type: none"> <li>1. Workstation networking is improperly configured.</li> <li>2. UTP cable connection is faulty.</li> <li>3. Failure to pass Ethernet packets.</li> </ol>	<ol style="list-style-type: none"> <li>1. Reset both Access Point and Station Adapter.</li> <li>Re-establish network connection.</li> <li>Verify proper workstation network configuration.</li> <li>2. Try to ping the remote network. Failure to detect the network may indicate a failure to pass Ethernet packets.</li> <li>3. Verify UTP cable connection. Solid LINK LED in workstation NIC indicates proper Ethernet connection.</li> <li>4. Check monitor messages for errors or other indications of problems.</li> <li>5. Check station counters to verify increase in Ethernet counters which indicates Ethernet activity.</li> </ol>

Problem and Indication	Possible Cause	Corrective Action
High quality signal but throughput is poor.	<ol style="list-style-type: none"><li>1. Too much interference or multipath propagation.</li><li>2. Ethernet port of the unit may be faulty.</li></ol>	<ol style="list-style-type: none"><li>1. Move the unit or the antennas out of the range of interference.  Check counters to see if more than 10% of total transmitted frames are retransmitted fragments.  Check if more than 10% of total received data frames are bad fragments.</li><li>2. Verify Ethernet port activity by checking Ethernet counters.</li></ol>
Link signal quality low or not as good as expected (indoor installation).	<ol style="list-style-type: none"><li>1. Possible multipath or structural interference.</li></ol>	<p>Reposition the unit outside range of possible interference.</p> <p>Check for heavy metal structures (e.g. elevators, racks, file cabinets) near unit.</p> <p>Check counters for excessive retransmissions or received bad fragments.</p> <p>Site may require higher gain antennas.</p> <p>Site may require a multicell structure (multiple AP units) due to multipath/structural interference.</p>
Link signal quality low or not as good as expected (outdoor installation).	There may be a problem with certain aspects of outdoor installation considerations (see relevant section in this manual).	<p>Verify that there is a clear line-of-site.</p> <p>Verify antenna height.</p> <p>Verify antenna polarization.</p> <p>Verify antenna alignment.</p> <p>Check length of cable between antenna and unit (an overly long extension cable may adversely affect performance).</p>

Problem and Indication	Possible Cause	Corrective Action
Unit associates with the wrong Access Point.	In a multicell structure with overlapping cells, the units may not associate with the closest Access Point.	For a unit to associate with a specific Access Point, assign a unique ESSID to the Access Point and to all the units you want to include in that wireless network.
Reduced performance in a multi-AP configuration.	The APs in the same coverage area have not been assigned unique hopping sequences.	Assign a unique hopping sequence to each AP in the coverage area. Each AP must have a unique hopping sequence regardless of ESSID.
Rx / Tx calibration error messages.	Auto Calibration is enabled for a "DE" unit.	Disable Auto Calibration for the unit.

# Checking Counters

Checking counters is also a good way to pinpoint any problems that may occur in the BreezeNET wireless LAN. Counters can be checked from the monitor.

## WLAN Counters

When checking WLAN counters, total retransmitted fragments should be below 10% of total transmitted (bridge) frames. If total retransmitted fragments are above 10%, this indicates errors in data transmission. Too many retransmissions may be an indication of interference between the transmitting and receiving units. Also, the ratio between Frames Dropped (too many retries) and Total Transmitted Frames (Bridge) should not exceed 1:40 (2.5%)

Received bad fragments should be no more than 10% of the total received data frames. If more than 10% of the total received data frames are bad fragments, this may indicate that there is a problem with the wireless link.

Refer to the previous *Troubleshooting Guide* section for possible corrective action.

## Ethernet Counters

When checking the Ethernet counters, received bad frames should be zero (0). If this is not the case, this may indicate a problem with the Ethernet connection. Verify Ethernet port link at hub, workstation, and unit. Assign a unique IP address to the unit and ping.







# Appendix A

## Combined Appendices

### About This Appendix

This appendix includes the following sections:

- ♦ **Supported MIBs and Traps**, page A-2, lists MIBs and traps supported by BreezeNET PRO.11 series products.
- ♦ **Technical Specifications**, page A-24, lists product and attachment specifications.
- ♦ **Wireless LAN Concepts**, page A-34, provides an overview of the concepts related to wireless LANs.
- ♦ **Radio Signal Propagation**, page A-43, discusses the concepts and applications of radio signal propagation relevant to wireless LANs.
- ♦ **IEEE 802.11 Technical Tutorial**, page A-53, introduces the new IEEE 802.11 standard.

# Supported MIBs and Traps

This chapter lists MIBs and traps supported by BreezeNET PRO.11 series products.

## Supported MIBs

All products in the BreezeNET PRO.11 series, as well as the Extended Range Access Point (AP-10 DE) and Workgroup Bridge (WB-10 DE), contain an embedded SNMP (Simple Network Management Protocol) agent. All functions can be accessed from the Management Information Base (MIB) using an SNMP application. IP host software

BreezeNET PRO.11 series agents support the following MIBs:

- ◆ MIB-II (RFC1213)
- ◆ BRIDGE-MIB (RFC1286)
- ◆ BreezeCOM Private MIB

The BreezeCOM Private MIB can be viewed by opening the MIB file on the provided diskette.

The following table provides a detailed description of all the supported MIBs and a short description of each.

	MIB	Name and Description
BrzSys	sysCmd	sysReset - Setting the value of this attribute to ON is interpreted as a system reset command.
		SysSetDefaults - Setting the value of this attribute to ON causes the system to set the NVRAM parameters to the factory default values. These values will become active after the next system reset.

	MIB	Name and Description
		sysSetPartialDefaults - Setting the value of this attribute to ON causes the system to set the partial NVRAM parameters to the factory default values. These values will become active after the next system reset.
		sysResetCounters - Setting the value of this attribute to ON causes the system to clear the performance counters.
		sysResetCounters - Setting the value of this attribute to ON causes the system to clear the performance counters.
		sysTrapEnable - Setting the value of this attribute to OFF disables the system from sending traps.
		sysTrapCounter - This attribute counts the total number of traps generated by the device since initialization.
		SysCarrierSense - This attribute defines the carrier sense absolute threshold.
		sysDeltaCarrierSense - This attribute defines the carrier sense differential threshold.
		sysRunFromNonActiveCode - This attribute forces you to run from non active code if the last is valid.
		<p>AccessRights</p> <p>sysDisplayAccessRights - This attribute displays the access rights of the station.</p> <p>SysChangeRightsToUSER - This attribute allows you to change the access rights of that station to USER. Type any string other than NULL to change the access right to user.</p> <p>SysChangeRightsToINSTALLER - This attribute allows you change the access rights of that station to INSTALLER. Type the password for the desired access right.</p> <p>SysChangeRightsToTECHNITIAN - This attribute allows you change the access rights of that station to AUTHORIZED TECHNICIAN. Type the password for the desired access right.</p>

	MIB	Name and Description
		SysChangeInstallerPassword - This attribute allows you change the Installer Password of that station. Type the new password, maximum 8 characters.
	SysParams	brzHWMacAddress - The Hardware MAC address of the device.
		BrzApplTunneling - This attribute specifies the device tunneling mode, as follows: IPX - the device will enable IPX tunneling only. Apple_Talk - the device will enable AppleTalk tunneling only. None - the device will disable tunneling. Both - the device will enable only IPX and AppleTalk tunneling.
		BrzPositiveBrg - This attribute specifies the Wired to Wireless LAN bridging mode at the AP, as follows: Reject_Unknown - the AP forwards to the Wireless LAN only frames that are destined to associated stations. Forward_Unknown - The AP forwards to the Wireless LAN frames destined to associated and unknown addresses. This value should be used only for Wireless Bridge installations. Intelligent - If connected to a wireless bridge, the AP automatically activates the Forward_Unknown option. NA - not applicable value, for non-AP devices.
		brzIpFilter - Setting the value of this attribute to ON will cause the system to filter all non-IP traffic to the Wireless LAN. This should be used on environments where only IP (and ARP) traffic is permitted. This option is available only on AP (NA value assigned in non-AP devices).
		brzTranslationMode - When this attribute is set to ON, data frames are translated for the Wireless LAN transmission. If it is set to OFF, tunneling of data frames applies. All devices within the same Wireless LAN network must have the same brzTranslationMode assigned.
		BrzWIXSupport - This attribute applies to installations with co-located APs. When it is set to ON, a load balancing algorithm is activated, resulting in balanced Basic Service Sets (cells). This option may be set only at some of the stations in the network.
		BrzWlanNetID - This attribute identifies the Wireless LAN network name (Extended Service Set ID) for that device. Stations are not allowed to associate to APs with different Net IDs.

	MIB	Name and Description
		BrzAuthenticationType - This attribute indicates the authentication algorithm used during the authentication sequence. The value of this attribute is one of the following: 1 - Open System, 2 - Shared Key 20 - Special Authentication Algorithm (#0) 21 - Special Authentication Algorithm (#1) 22 - Special Authentication Algorithm (#2)."
		BrzWlanRTNetID - This attribute identifies the run-time Wireless LAN network name (Extended Service Set ID) for that device. Stations are not allowed to associate to APs with different Net IDs.
		BrzApRedundancySupport - Setting the value of this attribute to ON will cause the Access-Point to discontinue sending beacons to the Wireless LAN after no multicast or unicast frames for the cell arrive from the Ethernet during a period of 100 seconds. This option is available ONLY on APs (a NA value is assigned in non-AP devices).
		brzWlanRelayUnicast - This attribute enables the relaying of unicast frames on the WLAN within the BSS. Setting this attribute to OFF means that unicast frames received from the WLAN by the AP can only be passed to the Distribution System. Applicable only in AP's.
		brzWlanRelayBroadcast - This attribute enables the relaying of broadcast frames on the WLAN within the BSS. Setting this attribute to OFF means that broadcast frames received from the WLAN by the AP can only be passed to the Distribution System. Applicable only in APs.
		brzApRedundancyLimit - This attribute sets the time limit, after which an Access-Point discontinues sending beacons to the Wireless LAN when no multicast or unicast frames for the cell arrive from the Ethernet. This option is available ONLY on AP (NA value assigned in non-AP devices).
		brzStaNumForLargeCW - This attribute sets the minimum number of stations in this cell that will cause this unit to use large CW; otherwise the unit will use the default CW. (The value is in the range of 1-120.)
		brzPowerMngMode - This attribute describes the current power management mode of the station. The allowed values are ACTIVE (for normal mode of operation), and POWER SAVE. An STA will always return an ACTIVE value.

	MIB	Name and Description
		BrzACKDelayed - This attribute applies to installations with co-located APs. When set to ON, a load balancing algorithm is activated, resulting in balanced Basic Service Sets (cells). This option may be set only at some of the stations in the network.
		BrzDTIMPeriod - ACCESS read-write STATUS mandatory description. This attribute defines the rate of DTIM frames. The value is expressed in Beacon Intervals. This attribute is applicable only in APs.
		brzPowerMngBitTestMode - This attribute describes the current power management bit test mode of the AP. The allowed values are DISABLED (for normal mode of operation) and ENABLED.
		BrzBeaconInterval - This attribute defines the rate of Beacon frames. The value is expressed in Dwells. This attribute is applicable only in APs.
		brzPowerSaveSupport - This attribute defines the power save support. 0 - Power Save support disabled 1 - Power Save support enabled 2 - Enable Power Save support with PM bit test This attribute is applicable only in APs.
		brzWlanAssocAge - This attribute defines the Association Aging Period.
		BrzDisplayRights - This attribute displays the current rights of the device.
		BrzNonActiveCodeState - This attribute displays the current non active code state. Warning! Activating this attribute will cause substantial degradation in station throughput. Respond rate is also delayed.
		BrzDisplayNonActiveCodeVersion - This attribute displays the current non active code version.
		brzIntelligentBridgingPeriod - This attribute defines the Intelligent Bridging Period in seconds.

	MIB	Name and Description
	IpParams	trapHostsTable - A list of trap_hosts entries.
		<p>TrapHostsEntry - A trap-receiving host entry, containing trap-host objects for a particular host.</p> <p>TrapHostsIndex - A unique value for each trap_host. Its value ranges between 1 and 3.</p> <p>TrapIPAddress - The IP address of the host to be sent all traps.</p> <p>TrapCommunity - The community of the host to be sent all traps.</p>
		IpAddr - The IP address of this device, used to access the device through any of its LAN Ports (Ethernet or WLAN).
		MaskIP - The IP Network mask used by the IP entity when accessing devices through any of its LAN Ports (Ethernet or WLAN).
		ReadCommunity - The device read community. If updated, it will be used after the next reset.
		WriteCommunity - The device write community. If updated, it will be used after the next reset.
		GatewayIPAddr - Gateway default IP address.
		BrzIPStack - This attribute defines whether to use the IP stack or not.
	BrzWlanParams	brzMaxRate - This attribute indicates the rate (in Mbits per second) at which data will be transmitted across the medium. The default value is 3.
		brzMobilLvl - This attribute indicates the expected mobility level of the system. The default value of this attribute is stationary.
		brzAvrgRssi - A value representing the average Signal Strength for packets received from the current AP. This attribute is applicable only for a station (an AP will always return a value of 255).
		BrzWlanProtocol - This attribute specifies the MAC/PHY protocol utilized by this system. This attribute is not write accessible for regular users.

	MIB	Name and Description
		BrzWlanTrapThreshold - This attribute specifies a threshold value for sending the WlanStatusTRAP. When the Wireless LAN quality drops below (or goes above) this value, a trap will be issued.
		BrzWlanQuality - A measure for quality (and noise level) of the Wireless LAN.
		BrzLastBeacon - A value representing the last dwell to receive beacons from that AP.
		BrzBadBeacons - A value representing the number of beacons received with a strength less than the join level from that AP.
		BrzLoadStations - A value representing the number of stations associated with that AP.
		KnownAPsTable - aKnownAPs in dot11, with additional quality information. A table of identities of the most recently known Access Points, and their signal quality.
		<p>KnownAPsEntry - An entry in the known APs table.</p> <p>knownAPsIndex - A unique value, representing the index of the AP in the Known APs table</p> <p>knownAPsValue - This attribute specifies the address of a recently known AP. The default value of this attribute shall be null (an empty entry).</p> <p>KnownAPsQuality - This attribute specifies the current reception quality of frames transmitted by that AP. At a station, a GOOD value indicates that the station can join that AP.</p> <p>KnownAPsAvrgRssi - A value representing the average Signal Strength for packets received from that AP.</p> <p>KnownAPsStatus - The validity of the current entry, either invalid or valid.</p> <p>KnownAPsLoadStations - A value representing the number of stations associated with that AP.</p>



	MIB	Name and Description
		<p>KnownAPsGoodBeacons - A value representing the number of beacons received with Strength more then join level from that AP.</p> <p>KnownAPsTotalBeacons - A value representing the total number of beacons (good and bad) received from that AP.</p>
	BssInfo	bssNumOfStations - This attribute specifies the number of devices that are currently associated with this AP.
		BssNumOfStationsPeak - This attribute contains the maximum value that bssNumOfStations has reached.
		TBD - This attribute contains the total beacons sent counter.
		<p>BssCollectPerStationInfo - When this attribute is set to ON, the AP accumulates Wireless Link statistics per station. This option is available only for the AP. At stations, it is always assigned with a NA (Not Applicable) value.</p> <p>Warning! Setting this attribute to ON can cause substantial degradation in cell throughput.</p>
		bssNumOfBeaconLost - This attribute contains the total beacons lost counter.
		BssNumOfStationsAuthenticated - This attribute specifies the number of devices, that are currently authenticated with this AP.
		BssNumOfStationsAuthenticatedPeak - This attribute contains the maximum value that bssNumOfStationsAuthenticated has reached.
	BssApAdb	adbTable - A table of the associated stations.
		AdbEntry - An entry in the ADB table.
		stAddress - The MAC Address of the station represented by this entry in the Association Data Base.
		StCFMode - This attribute is set to ON if the station is in the Contention Free Polling list of the AP.

	MIB	Name and Description
		StMaxRate - This attribute indicates the maximum rate (in Mbits per second) at which that station transmits data across the Wireless medium.
		StCurTxRate - The rate currently used by the AP to transmit packets to this station.
		StRssi - A value representing the average Signal Strength for packets received from that station. This attribute is updated only if sysCollectPerStationInfo is set to ON.
		StPMMMode - The current Power Management mode of this station.
		StTxFragments1M - This attribute counts the total number of fragments (including retransmissions), that were transmitted to that station over the Wireless LAN in 1Mbps. It is updated only if sysCollectPerStationInfo is set to ON.
		StTxFragments2M - This attribute counts the total number of fragments (including retransmissions), that were transmitted to that station over the Wireless LAN in 2Mbps. It is updated only if sysCollectPerStationInfo is set to ON.
		StTxFragments3M - This attribute counts the total number of fragments (including retransmissions), that were transmitted to that station over the Wireless LAN in 3Mbps. It is updated only if sysCollectPerStationInfo is set to ON.
		StTxRetry - This attribute counts the total number of retransmissions to that station over the Wireless LAN. It is updated only if sysCollectPerStationInfo is set to ON.
		StTxDroppedPackets - This attribute counts the number of transmit frames (data or management) to this station that were dropped because of too many retransmissions. It is updated only if sysCollectPerStationInfo is set to ON.
		StRxFragments - This attribute counts the total number of fragments (data and management) that have been received successfully from that station through the Wireless LAN. It is updated only if sysCollectPerStationInfo is set to ON.

	MIB	Name and Description
		StWlanStatus - This attribute specifies the current reception quality of frames, transmitted by that station.
		StResetCounters Setting the value of this attribute to ON will clear the station counters at the AP (clear the counters in that adbEntry). Warning! Setting the value of this attribute to ON may cause momentary degradation in performance.
		stType - This attribute identifies the device type of the station.
	BrzSTA	brzCurrentAPMacAddress - The hardware MAC address of the AP currently associated with. Available ONLY in station.
		BrzLastAPMacAddress - The hardware MAC address of the last AP that the station was associated with. Available ONLY in stations.
		BrzPreferredAPMacAddress The hardware MAC address of the preferred AP, to which the station should associate whenever possible. Null value here indicates no preference. Available ONLY in stations.
		BrzRoamToAPMacAddress - Setting this attribute to a specific AP MAC address will cause the station to roam immediately to that AP, if possible. Available ONLY for stations.
		brzCFMode - This attribute is set to ON if the station required Contention Free services from the AP (hence it is in the AP's Contention Free list). This option is available ONLY on stations. A NA value is returned for all APs.
		brzTx1MBitRate - Total transmitted frames in 1 MBit rate.
		brzTx2MBitRate - Total transmitted frames in 2 MBit rate.
		brzTx3MBitRate - Total transmitted frames in 3 MBit rate.
		BrzTotalRetx - Total Retransmitted frames including all rates.
	BrzRoamParams	brzRoamDecisionWin - This parameter defines a minimum number of RSSI samples which is required to make a decision about the current WLAN channel quality. A new RSSI sample arrives with each incoming frame. Available ONLY in stations.

	MIB	Name and Description
		BrzRoamDecisionNumerator - This parameter defines the maximum number of RSSI samples that are allowed to be below brzRoamDecisionRSSIThreshold, among a number equal to brzRoamDecisionWin of the last arrived samples. If a number of bad samples (i.e. below brzRoamDecisionRSSIThreshold) exceeds this parameter setting, the channel is considered to be BAD. Available ONLY in stations.
		BrzRoamDecisionRSSIThreshold - If an RSSI sample is bellow the value which is defined by this parameter the sample is considered to be BAD. Available ONLY in stations.
		BrzJoinDecisionRSSIThreshold - A station will join a new AP only if the AP transmits with an RSSI quality above the value which is defined by this parameter. Available ONLY in stations. In AP's, this is the threshold for sending Bad WLAN Conditions traps. If a station associated with the AP is heard at an RSII level below this threshold, a Bad WLAN Conditions trap is sent by the AP.
		BrzNeighboringBeacons - This parameters defines once in how many dwell times the AP will send a neighboring beacon. Available ONLY in AP's.
		brzNumberOfProbeResponses - If a number of good RSSI samples coming from a neighbor is greater than or equal to this parameter, the neighbor might be selected for joining.
		BrzNumberOfBeaconsForDisconnect - This parameter defines the maximum number of consecutive not arrived Beacons allowed before a disconnect decision. Available ONLY in stations.
		BrzMaxNumberOfScanning - This parameter defines a maximum number of scanning attempts to perform before system reset. A value of zero implies non reset. Available ONLY in stations.
		BrzNeighboringBeaconRate - This parameter defines the Neighboring Beacon Rate in dwells. A value of zero implies non Neighboring Beacons. Available ONLY in AP's.
brzCnt	brzDSCnt	brzRxFromDS - This attribute counts the total number of frames that have been received successfully from the Wired Distribution system.

	MIB	Name and Description
		BrzRxBadFromDS - This attribute counts the number errored frames, received from the Wired Distribution system.
		BrzRxOctetsFromDS - This attribute counts the total number of octets that have been received successfully from the Wired Distribution system.
		BrgbrzMissedFrames - This attribute counts the total number of missed frames that have missed the transmission to the Ethernet LAN.
		BrzTxToDS - This attribute counts the total number of frames that have been transmitted to the Wired Distribution system.
	BrzWlanCnt	brzTxWlanCnt - brzTxPacketsToWlan - This attribute counts the total number of frames (data and management) that have been transmitted to the Wireless LAN.
		BrzTxMSDUToWlan - This attribute counts the total number of frames (data frames) that have been transmitted to the Wireless LAN.
		BrzDiscarded - This attribute counts the number of data frames that were internally discarded in the system, instead of being transmitted over the Wireless LAN. High values of this counter indicate either very high traffic volume, or a noisy environment that prevents Wireless transmissions.
		BrzTxFragToWlan - This attribute counts the total number of fragments (including retransmissions), that were transmitted to the Wireless LAN.
		BrzRetryOnWlan - This attribute counts the total number of retransmitted fragments on the Wireless LAN.
		BrzFailedCountOnWlan - Equals to the dot11 FailedCount. This attribute counts the number of frames that were dropped (not transmitted), due to the number of retransmit attempts exceeding the RetryMax value.
		BrzTxErrorAckTimeOut - This attribute counts the total number of acknowledge timeouts on the Wireless LAN.
		BrzTxErrorAckCRC - This attribute counts the total number of acknowledge CRC errors on the Wireless LAN.

	MIB	Name and Description
		BrzTxErrorNoTimeUntilHop - This attribute counts the total number of timeouts until end of the hop on the wireless cell.
		BrzTxErrorUnderRunAndCTS - This attribute counts the total number of errors caused by hardware problems (Under Run).
		BrzTxErrorAbort - This attribute counts the total number of errors caused by frame abortion from Boori.
		BrzTxErrorFrameReceived - This attribute counts the total number of errors caused by frame failure on the Wireless LAN.
		BrzRxWlanCnt - brzRxPacketsFromWlan - This attribute counts the total number of frames (data and management) that have been received successfully from the Wireless LAN.
		BrzRxMSDUFromWlan - This attribute counts the total number of MSDUs (data frames) that have been received successfully from the Wireless LAN.
		BrzRxFragFromWlan - Equals to the dot11 ReceivedFrameCount. This attribute counts the number of fragments (data and management), that have been received successfully from the Wireless LAN.
		BrzRxBadFragFromWlan - This counter is incremented when an error is detected in a fragment received from the Wireless LAN.
		BrzRxDuplicateFragFromWlan - Equals to the dot11 FrameDuplicateCount. This counter is incremented when a duplicated fragment is received from the Wireless LAN.
		FreqStatisticsTable - A table for the traffic statistics of each frequency.
		<p>FreqStatisticsEntry - An entry in the Frequencies Statistics table.</p> <p>freqStatisticsIndex - A unique value representing the index of the frequency in the hopping sequence table</p> <p>freqNo - This attributes specifies the channel number of the frequency for which this entry accumulates the statistics.</p>

	MIB	Name and Description
		FreqTotalReceived - This attribute counts the total number of frames (data and management) that have been received successfully from the Wireless LAN in that specific frequency.
	BrzRoamCnt	brzNumOfReassocRequests - For an AP: The number of Association and Reassociation requests received since the last reset of the AP. This counter is useful for getting information about mobility activity on the BSS. For a Station: The number of Associations and Reassociation requests issued by the station since the last reset.
	BrzMngCnt	brzMngAP - ProbeResponseSent - For an AP: Number of Probe response that sent
		ProbeResponseLost - For an AP: Number of Probe response that got lost.
		ProbeResponseSentRetx - For an AP: Number of retransmitted Probe response frames that sent.
		AssocResponseSent - For an AP: Number of Association Probe response frames that sent.
		AssocResponseLost - For an AP: Number of Association Probe response frames that got lost.
		AssocResponseSentRetx - For WB or SA: Number of retransmitted Association Probe response frames that sent.
		BrzMngSAWB - ProbRequestSent - For WB or SA: Number of Probe request frames that sent.
		AuthRequestSent - For WB or SA: Number of Authentication request frames that sent.
		AuthRequestSentRetx - For WB or SA: Number of Retransmitted Association request frames that sent.
		AssocRequestSent - For WB or SA: Number of Association request frames that sent.

	MIB	Name and Description
		AssocRequestSentRetx - For WB or SA: Number of Retransmitted Association request frames that sent.
	BrzPSCnt	PSFreeEntries - For an AP: Number of station free entries.
		PSInternallydiscarded - For an AP: Number of Internally Discarded frames.
		PSstations - For an AP: Number of power saved station connected to this AP.
		PSPowerSavingAged - For an AP: Number of frames that were not transmitted due to the end of aging time.
		PowreStationsTable - A list of trap_hosts entries.
		<p>PowreStationsEntry - A trap-receiving host entry, containing trap-host objects for a particular host.</p> <p>PowerSaveIndex - A unique value, representing the index of the frequency in the hopping sequence table</p> <p>powerSaveStationID - The identifier numerator of the Station in the AP. Note: ID zero is Broadcast.</p>
		PowerSaveBuffered - This attribute specifies how many messages are waiting for that station in the AP buffers.
		PowerSaveAged - This attribute specifies how many stations were deleted after a long waiting time.
		PowerSaveSent - This attribute specifies how many messages were sent to that station.
		PowerSaveQueueFull - This attribute specifies how many messages were discarded because the queue to that station was full.
	BrzTraps	brzTrapAPMacAddr - The MAC address of an AP.
		BrzTrapSTAMacAddr - The MAC address of a station device.



	MIB	Name and Description
		BrzTrapMacAddress - A STA or AP MAC address.
		BrzTrapRssiQuality - The RSSI level of the signal received from the Access Point.
		BrzTrapLastRssiQuality - The RSSI level of the signal received from the previous Access Point.
		BrzTrapIndex - Index number for future trap implementation.
		BrzTrapText - Textual string for future trap implementation.
		BrzTrapToggle - A general ON/OFF toggle value, for the traps.
		BrzTrapSTAType - This attribute identifies the device type of the station.
		BrzAProamingInTRAP - A trap indicating that a station has roamed into this AP. It contains the MAC address of the associated station and the device type of that station.
		BrzAPassociatedTRAP - An AP trap indicating that a new station was associated with this AP. It contains the MAC address of the associated station.
		BrzAPdisassociatedTRAP - An AP trap indicating that the station disassociated itself from the AP. The trap contains the MAC address of the disassociated station.
		BrzAPagingTRAP - An AP trap indicating that the station association was aged out, and removed from that AP. The trap contains the MAC address of the aging station.
		BrzAProamedOutTRAP - An AP trap indicating that a given station has roamed out from this AP. The trap contains the MAC address of the roamed out station.
		BrzSTAassociatedTRAP - A station trap, indicating that the station became associated-with, or has roamed-to, another AP. The trap contains the MAC address and the average RSSI level of the new AP. If the station was roaming, the MAC address of the old AP, and the RSSI level prior to roaming, is also provided (for an association, the second address will appear as all-zeros).

	MIB	Name and Description
		BrzWlanStatusTRAP - An AP and STA trap, indicating a change in the conditions of the wireless media. An ON value is sent when the Wireless LAN quality drops below the brzWlanTrapThreshold value. A trap with an OFF value is sent if the quality improves, exceeding the brzWlanTrapThreshold value. The Wireless LAN quality value is also sent.
		BrzWlanStatusOfStationTRAP - An AP trap, indicating a change in the quality of the Wireless connection, with a specific (associated) station. An ON value indicates an especially bad connection, and an OFF value is sent if the quality improves, exceeding a predetermined threshold value. The brzTrapMacAddress contains the MAC address of the applicable station.
		BrzGeneralTRAP - An AP and STA general purpose trap, for future trap implementation.
	brzdot11	dot11smt - dot11DefaultWEPKey1 - This attribute indicates the WEP secret key value corresponding to KeyID 1. The WEP secret key is logically WRITE-ONLY. Attempts to read this attribute shall return a string of asterisks (enter exactly 10 Hex-Decimal digits).
		dot11DefaultWEPKey2 - This attribute indicates the WEP secret key value corresponding to KeyID 2. The WEP secret key is logically WRITE-ONLY. Attempts to read this attribute shall return a string of asterisks (enter exactly 10 Hex-Decimal digits).
		dot11DefaultWEPKey3 - This attribute indicates the WEP secret key value corresponding to KeyID 3. The WEP secret key is logically WRITE-ONLY. Attempts to read this attribute shall return a string of asterisks (enter exactly 10 Hex-Decimal digits).
		dot11DefaultWEPKey4 - This attribute indicates the WEP secret key value corresponding to KeyID 4. The WEP secret key is logically WRITE-ONLY. Attempts to read this attribute shall return a string of asterisks (enter exactly 10 Hex-Decimal digits).
		dot11PrivacyGrp - dot11PrivacyOptionImplemented - This attribute, when true, indicates that the 802.11 WEP option is implemented.

	MIB	Name and Description
		dot11PrivacyInvoke - This attribute indicates if a special mechanism is invoked, to protect the Wireless LAN transmissions. The value is one of the following: 1 - Standard WEP, 2 - No Encryption, 20 - Special Encryption (#0), 21 - Special Encryption (#1), 22 - Special Encryption (#2)
		dot11WEPDefaultKeyID - This attribute indicates the use of the first, second, third or fourth DefaultWEPKey when set to values of one, two, three or four.
		dot11Preauthentication - This attribute, when true, enables Pre-authentication algorithm.
	dot11OperationGrp	dot11RTSThreshold - This attribute indicates the number of bytes in an MPDU (frame), above which an RTS/CTS handshake will be performed. Setting this attribute to be larger than the maximum frame size, will prevent the RTS/CTS handshake for frames transmitted by this station.
		dot11ShortRetryLimit - This attribute indicates the number of retransmission attempts made, before a failure condition is indicated.
		dot11FragmentationThreshold - This attribute specifies the current maximum size, in octets, of the MPDU that will be delivered to the PHY. A frame will be broken into fragments if its size exceeds the value of this attribute, after adding MAC header and tail. The value is one of the following: 1 - 560 octets 2 - 800 octets 3 - 1518 octets
		dot11DwellRetryLimit - This attribute indicates the number of retransmission attempts made in several Dwells, before a failure condition is indicated. Values between 0 to 9.
		dot11MaxMulticastRate - This attribute indicates the basic rate for multicast frames.
		dot11DwellTime - This attribute indicates the dwell time in Kilo-microsecond. Allowed Values are between 19 to 390. This attribute is available only in AP's.

	MIB	Name and Description
	dot11res	dot11ResourceInfo - dot11manufacturerName - This attribute identifies the manufacturer of the resource.
		Dot11manufacturerProductName - This attribute identifies the manufacturer product name of the resource.
		dot11manufacturerProductVersion - This attribute identifies the manufacturer's product version of the resource.
		dot11CurrentStationStatus - This attribute identifies the current Station WLAN status.
		dot11TotalNumberOfAssocSinceLastReset - This attribute identifies how many time the device Associated since startup.
	dot11phy	dot11PhyOperationGrp - This attribute specifies the regularity domain, for the radio operation of this device. This integer contains an 8 bit value, as defined below: 00h - EthAirNet 10h - USA 20h - Canada 30h - Europe 31h - Spain 32h - France 37h - Europe Double Deviation 38h - Netherlands 40h - Japan 41h - Korea 48h - Israel 49h - Australia 60h - Proprietary
		dot11PhyAntennaGrp - dot11CurrentTxAntenna - This attribute specifies the current antenna being used to transmit. The value is one of the following: 0 - Intelligent antennas selection 1 - Transmitting only with antenna 1 2 - Transmitting always with antenna 2.
		dot11PhyTxPwrGrp - dot11CurrentTxPwrLvl. This attribute specifies the power level, currently being used to transmit data. The value is one of the following: 0 - Low or 1 - High.

	MIB	Name and Description
		dot11PhyFHSSGrp - dot11CurrentDwellTime OBJECT-TYPE This attribute specifies the current time, in Kilo-microseconds, that the radio operates on a single channel. The value is between 19 to 390. The same Dwell Time value should be assigned to all the devices within the same Wireless LAN network.
		dot11CurrentSet - This attribute represents the current set of patterns that the device is using to determine the hop sequence. The range of values is 1 to 3, and the default is 1.
		dot11CurrentPattern - This attribute represents the current pattern that the device is using to determine the hop sequence.
		dot11MultySupport - dot11MultyRateSupport - This attribute indicates the multi cast rate support.
		dot11MultyRateDecisionWindow - This attribute indicates the multi cast rate decision window size.
	dot11Maintenance	dot11WaitforAssociationAddress - This attribute indicates the station MAC address. 0 - Use mine 1 - Wait for update via Ethernet Available only for Stations
		dot11JapanCallSign - This attribute indicates the Japan call sign string. Available only for Japan standard.

## Supported Traps

The following traps are implemented by BreezeNET PRO.11 units. All BreezeNET PRO.11 units that have the SNMP Traps parameter enabled will send traps to the network's designated managers. The traps can be viewed and filtered using SNMPc.

To enable/disable trap sending for a device, use the *IP and SNMP Parameters* menu.

The following table lists the traps implemented by Alvarion PRO.11 units:

Trap	Variables	Description
brzAProamingIn	brzTrapSTAMacAddr	A station has roamed into this AP coverage area. The trap contains the MAC address of the associated station.
BrzAPassociated	brzTrapSTAMacAddr	A new station is associated with this AP. The trap contains the MAC address of the associated station.
BrzAPdisassociated	brzTrapSTAMacAddr	A station has disassociated itself from this AP. The trap contains the MAC address of the associated station.
BrzAPaging	brzTrapSTAMacAddr	A station association was aged out and removed from this AP. The trap contains the MAC address of the aged-out station.
BrzAProamedout	brzTrapSTAMacAddr	A station has roamed out of this AP's range. The trap contains the MAC address of the station that roamed out.

Trap	Variables	Description
BrzSTAassociated	brzLastAPMacAddr brzTrapAPMac brzTrapLastRssiQuality brzTrapRssiQuality	A station has become associated with, or roamed to, a new AP. The trap contains the MAC address and average RSSI level of the new AP ( <i>TrapAPMac</i> and <i>TrapRssiQuality</i> variables). If the station has been roaming, the MAC address of the old AP and the RSSI level prior to roaming are also provided ( <i>LastAPMacAddr</i> and <i>LastRssiQuality</i> variables). For an association, the second address appears as all zeros.
BrzWlanStatus	brzTrapToggle  brzTrapMacAddress	The wireless media condition has changed. An ON value is sent when the wireless LAN quality for a station or AP drops below the WLAN trap threshold. An OFF value is sent if the quality improves beyond the threshold. The current value of wireless LAN quality is also sent.
BrzWlanStatusOfStation	brzTrapToggle  brzTrapMacAddress	The quality of the wireless connection to the AP has changed. An ON value is sent when the connection goes lower than the predetermined threshold. An OFF value is sent when the quality improves above the threshold. The <i>brzTrapMacAddress</i> variable contains the MAC address of the applicable station.
BrzGeneral	brzTrapIndex  brzTrapText	For future use.

# Technical Specifications

## Specifications for BreezeNET PRO.11 Units

The following table provides the technical specifications for all products in the BreezeNET PRO.11 series.

Technical Specifications	AP-10 PRO. 11, SA-10/40 PRO. 11, WB-10 PRO. 11	SA-PCR PRO.11 SA-PCD PRO.11
<b>Wired LAN interface</b>		
Compliant with	Ethernet / IEEE 802.3 CSMA/CD standard	N/A
Physical Interface	10BaseT	PC card type II / PCMCIA 2.1
Network Operating Systems supported	All	Windows 95, 98, NT4
Network protocols supported	All	NDIS
<b>Wireless LAN interface</b>		
Compliant with	IEEE 802.11 CSMA / CA Wireless LAN standard	
Physical interface – two antennas	Integrated or External	
<b>Radio Specifications</b>		
Type	Frequency Hopping Spread Spectrum (FHSS)	
Frequency range	2.4 GHz – 2.4835 GHz (ISM band) (different ranges available for countries using other bands)	
Dwell time	1-255msec	



Technical Specifications		AP-10 PRO. 11, SA-10/40 PRO. 11, WB-10 PRO. 11	SA-PCR PRO.11 SA-PCD PRO.11
Transmitted power - integrated antennas		Up to 100 mW (20dBm) EIRP	
Transmitted power - external antennas		D models: - High Power (at the connector): 17dBm (50mW) - Low Power (at the connector): 10dBm (10 mW)	
Sensitivity:	@ 1 Mbps	–81dBm	
	@ 2 Mbps	–75dBm	
	@ 3 Mbps	–67dBm	
Modulation		Multilevel GFSK	
Demodulation Technology		DSP-based with adaptive equalization	
Antenna Diversity		Two antennas, selected for use on a packet basis	
Frequency Accuracy		+/- 10 PPM	
Approvals of Compliance		FCC part 15, ETS 300-328, UL, UL/C, TUV/GS, CE	
Configuration and Management			
Configuration and Setup		Via Local Monitor port (serial RS-232)	Via Application
SNMP management SNMP agents		MIB II, Bridge MIB, WLAN MIB, and private MIB	N/A
Access via		Wired LAN, Wireless LAN	

Technical Specifications	AP-10 PRO. 11, SA-10/40 PRO. 11, WB-10 PRO. 11	SA-PCR PRO.11 SA-PCD PRO.11
Site Survey	Via Local Monitor port (serial RS-232) Via SNMP	Via Application
Front Panel Display LED indicators	- Power on - Wired LAN activity - Wireless LAN synchronization - Wireless LAN signal quality/Load	- Link Status - Data Traffic
S/W upgradeable	Through TFTP download	via PC
<b>System Considerations</b>		
Range (Access Point to Station)	Depends on rate and antenna cable length/quality. (Accurate values must be calculated for specific installations).	
Range - unobstructed with integrated antennas	2000 ft. (600m)	1500 ft. (450m)
Range - unobstructed with external antennas (models D, DE and DL)	USA FCC - up to 6 miles Europe ETSI (DL model only) - up to 2.5 km Europe ETSI (DE model only) - up to 5 km Non-Regulated - 30 km and above	N/A
Range - Office Environment	Up to 500 ft. (150m)	
Maximum no. of APs per wired LAN	Unlimited	
Maximum no. of co-located (overlapping) cells (Access Points)	15	
Data Rate: over the air nominal net aggregate	1, 2, or 3 Mbps Up to 2 Mbps Over 5 Mbps with overlapped cells	
High Speed roaming	up to 60 mph (90 kph)	
Load sharing support	yes (with WIX™)	

Technical Specifications	AP-10 PRO. 11, SA-10/40 PRO. 11, WB-10 PRO. 11	SA-PCR PRO.11 SA-PCD PRO.11
Dynamic rate selection based on radio medium quality	Yes	
Electrical		
External Power Supply	100V - 250V, 50-60Hz, 0.5A	via network PC
Input Voltage	5Vdc	5Vdc
Power Consumption	1.5A (peak) 1.2A (average)	- XMT 365mA (peak) - RCV 280mA (peak)
Mechanical		
Dimensions (without antennas and power supply)	5.1” x 3.4” x 1.35” (13cm x 8.6cm x 3cm)	standard PCMCIA Type II
Weight (without antennas and power supply)	0.9 lb. (0.4 kg.)	1.1 oz (32 gr.)
Environmental		
Operating Temperature	32° F - 105° F (0° C - 40° C)	
Operating Humidity	5% - 95% non-condensing	

**NOTE:**

All specifications are subject to change without notice.

## Specifications for TPA 24 Transmit Power Amplifier

<b>Models used with the BreezeNET PRO.11 Series</b>	<ul style="list-style-type: none"><li>• TPA 24 NL</li><li>• TPA 24 NH</li></ul>
<b>Input Power</b>	<ul style="list-style-type: none"><li>• TPA 24 NL: -10dBm - 0dBm (Low input)</li><li>• TPA 24 NH: 0dBm - +10dBm (High input)</li></ul>
<b>Output Power</b>	24 dBm (250mW) (fixed output level)
<b>Input Impedance</b>	50W
<b>Output Impedance</b>	50W (DC short)
<b>Operating Temperature</b>	-20° to 50°C
<b>Power Requirements</b>	12V; 420 mA (Power Supply and Power Inserter are supplied with models TPA-24 NL and TPA-24 NH)
<b>Connectors</b>	<ul style="list-style-type: none"><li>• TPA 24: IN - N-type Male; OUT - N-type Female</li><li>• Power Inserter: RF - N-type Male; RF&amp;DC - N-type Female</li></ul>
<b>Dimensions</b>	70mm x 150mm x 25mm (2.8"x 6"x 1")
<b>Operating Environment</b>	<ul style="list-style-type: none"><li>• TPA 24 - For outdoor/indoor use</li><li>• Power Supply - For indoor use</li><li>• Power Inserter - For indoor use</li></ul>

**NOTE:**

All specifications are subject to change without notice.

## Specifications for LNA 10 Low Noise Receive Amplifier

<b>Gain</b>	10dB
<b>Noise Figure</b>	1.5dB Typ, 2dB Max.
<b>Response Flatness</b>	$\pm 1.5$ dB
<b>Max. RF Input Level</b>	-15dBm
<b>Input Impedance</b>	50W
<b>Output Impedance</b>	50W
<b>Connectors</b>	<ul style="list-style-type: none"> <li>•LNA-10: RF IN: N-type, female RF OUT: N-type, male Signal and Power IN: not in use Signal and Power OUT: F-type, female</li> <li>•Power Inserter: To CONV - F-type, female To TV - F-type, female</li> </ul>
<b>Power Supply: Required Voltage Required Current</b>	+12V to +28Vdc 20mA
<b>Operating Temperature</b>	-20° C to +50° C
<b>Dimensions</b>	60mm x 35mm x 25mm (2.3"x 1.3"x 1")
<b>Operating Environment</b>	LNA 10 - outdoor/indoor Power Supply - indoor Power inserter - indoor

### NOTE:

All specifications are subject to change without notice.

## Specifications for RFS 122 Radio Frequency Splitter

Insertion Loss	3.8dB max.
Isolation	19dB min.
Power Rating	10 W max.
Internal Load Dissipation	125 mW max.
Input Impedance	50W
Output Impedance	50W
Connectors	<ul style="list-style-type: none"><li>• SUM: N-type, Male</li><li>• PORTS: N-type, Female (on each port)</li></ul>
Operating Temperature	-20° C to +85° C
Dimensions	51mm x 51mm x 19mm (2" x 2" x 0.75")
Operating Environment	Outdoor/Indoor

## Specifications for AL 1 Lightning Arrestor

Turn on voltage	75V
Insertion loss	0.3dB typical
DC path from input to output	existing
Operating Temperature	-55° C to +70° C
Dimensions	67.5mm x 25mm x 25mm (2.7" x 1" x 1")
Connectors	<ul style="list-style-type: none"><li>• Antenna Port: N-type, Female</li><li>• Equipment Port: N-type, Female</li></ul>
Operating Environment	Indoor/Outdoor
Grounding	One of the female-type N connectors is mounted directly through a hole in the shelter wall and held in place with a lockwasher and nut.

**NOTE:**

All specifications are subject to change without notice.

## Specifications for AMP 2440 Bi-Directional Power Amplifier

General Specifications	
Operating Range	2400-2483 MHz
Operating Mode	Bi-directional, half-duplex. Senses RF carrier from transmitter and automatically switches from receive to transmit mode.
Connectors	N-female
Indicators	TX and RX LEDs on both the amplifier and the DC bias injector
Lightning Protection	Direct DC ground at antenna connector
DC Surge Protection	600 Watt TVS at 12 VDC input from transmission cable
Transmitter Amplifier	
Transmit Gain	Up to 15 dB
Frequency Response	+/-1 dB over operating range
Transmit Output Power	AMP 2440-500 model: 500 mW * AMP 2440-250 model: 250 mW.
Transmit Input Power	3 mW minimum, 100mW maximum (+3dBm required to cause TX mode)
Receiver Low Noise Amplifier (LNA)	
Receive Gain	18 dB typical



Frequency Response	+/-1 dB over operating range
Noise Figure	3.5 dB approximately
Third Order Intercept	20 dBm
<b>Mechanical and Environmental</b>	
Operating Temperature	-20°C to +60°C
Power	12VDC @ 650mA or 105-240 VAC from power supply provided with kit
Dimensions	Amplifier: 3.85" x 2.52" x 1.46" DC Power injector: 4.42" x 2.40" x 1.22"
Mounting Bracket for amplifier	Accommodates pole/mast diameters from 3/4" to 3"
Kit Weight	Approx. 1.5 lb. with U-bolts

# Wireless LAN Concepts

Wireless LAN technology is becoming increasingly popular in large-scale and complex wireless networks, as more and more users are discovering its reliability and high performance.

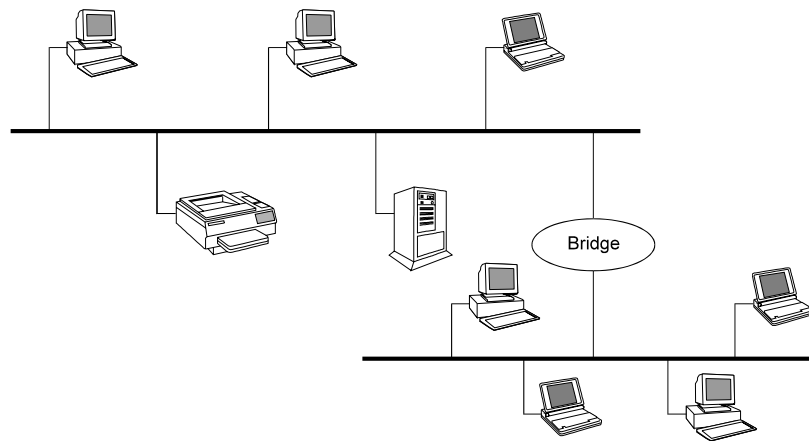
Originally designed for indoor office applications, today's wireless LANs can be used for both indoor client-server and peer-to-peer networks as well as for outdoor point-to-point and point-to-multipoint remote bridging applications.

Wireless LANs are designed to be modular and very flexible. They can also be optimized for different environments. For example, point-to-point outdoor links are less susceptible to interference and can have higher performance if designers increase the Dwell Time and disable the Collision Avoidance and Fragmentation mechanisms described later in this section.

## Topology

### Wired LAN Topology

Traditional LANs (Local Area Networks) link PCs and other computers to one another and to file servers, printers and other network equipment using cables or optic fibers as the transmission medium.

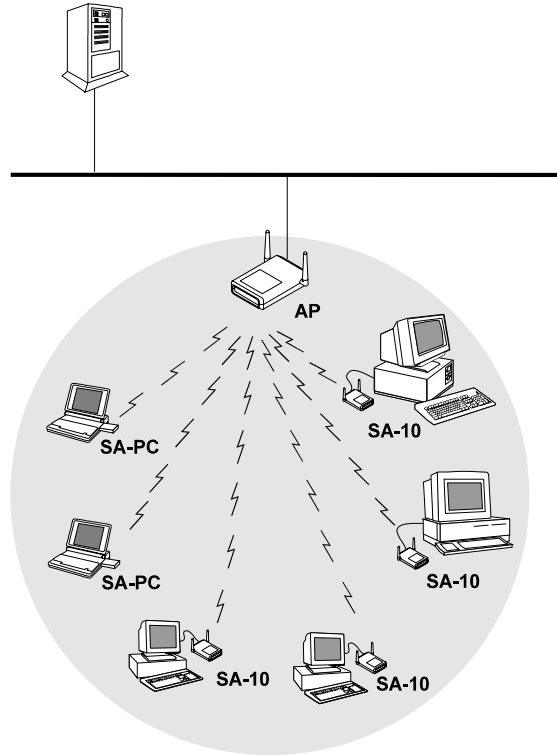


**Figure A-1: Wired LAN Topology**

### Wireless LAN Topology

Wireless LANs enable workstations to communicate and access the network using radio propagation as the transmission medium. Wireless LANs can be connected to existing wired LANs as an extension, or can form the basis of a new network. While adaptable to both indoor and outdoor environments, wireless LANs are especially suited to indoor locations such as office buildings, manufacturing floors, hospitals and universities.

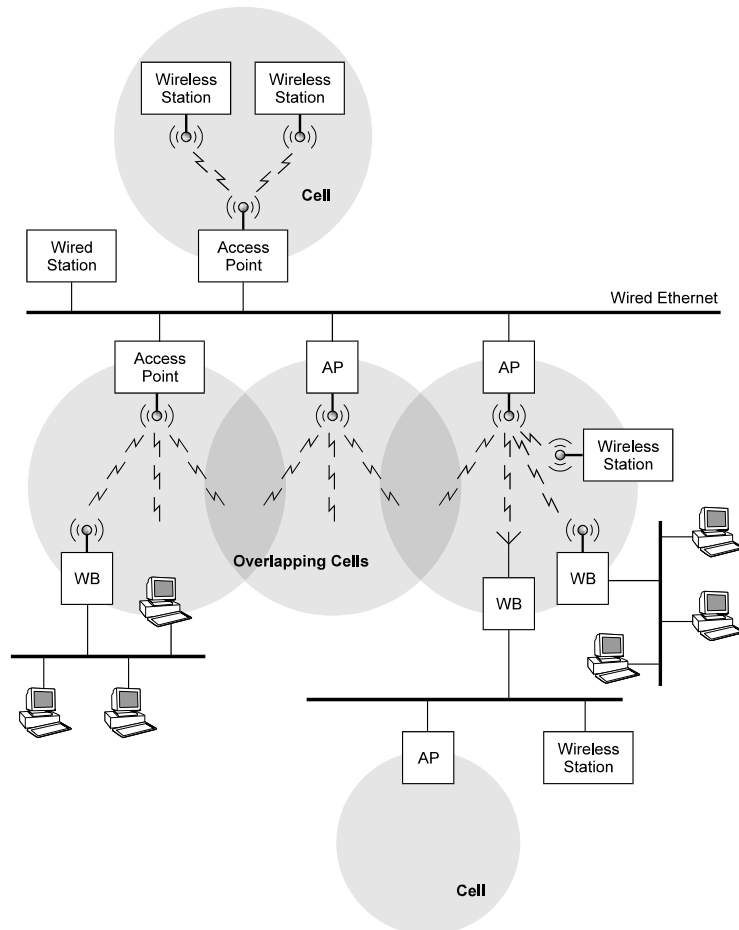
The basic building block of the wireless LAN is the Cell. This is the area in which wireless communication takes place. The coverage area of a cell depends on the strength of the propagated radio signal and the type and construction of walls, partitions and other physical characteristics of the indoor environment. PC-based workstations, notebook and pen-based computers can move freely in the cell.



**Figure A-2: The Basic Wireless LAN Cell**

Each wireless LAN cell requires some communications and traffic management. This is coordinated by an Access Point (AP) which communicates with each wireless station in its coverage area. Stations also communicate with each other via the AP, so communicating stations can be hidden from one another. In this way, the AP functions as a relay, extending the range of the system.

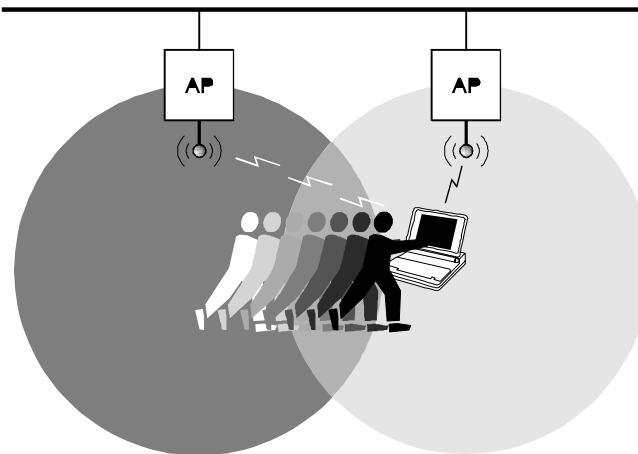
The AP also functions as a bridge between the wireless stations and the wired network and the other wireless cells. Connecting the AP to the backbone or other wireless cells can be done by wire or by a separate wireless link, using wireless bridges. The range of the system can be extended by cascading several wireless links one after the other.



**Figure A-3: Wireless LAN Connectivity**

## Roaming

When any area in the building is within reception range of more than one Access Point, the cells' coverage is said to overlap. Each wireless station automatically establishes the best possible connection with one of the Access Points. Overlapping coverage areas are an important attribute of the wireless LAN setup, because this enables seamless roaming between overlapping cells.

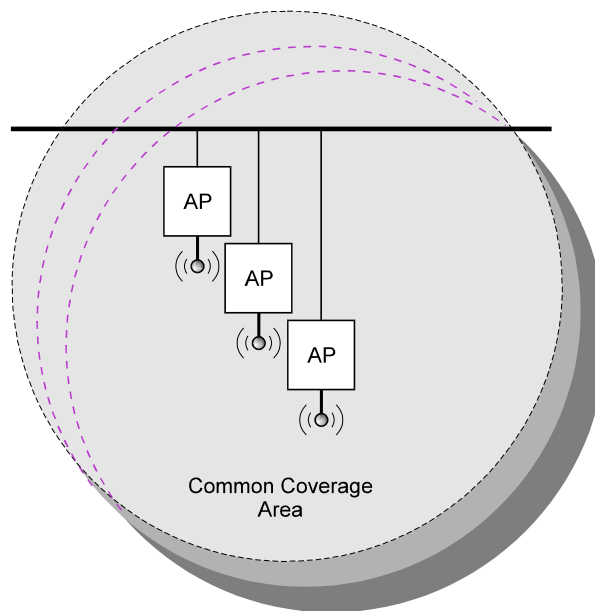


**Figure A-4: Roaming Through Overlapping Cells**

Roaming allows mobile users with portable stations to move freely between overlapping cells, constantly maintaining their network connection. Roaming is seamless: a work session can be maintained while moving from one cell to another. Multiple Access Points can provide wireless coverage for an entire building or campus. When the coverage area of two or more APs overlap, the stations in the overlapping area can establish the best possible connection with one of the APs, continuously searching for the best AP. In order to minimize packet loss during switch-over, the “old” and “new” APs communicate to coordinate the process.

## Load Sharing

Congested areas with many users and heavy traffic load per unit may require a multi-cell structure. In a multi-cell structure, several co-located APs “illuminate” the same area creating a common coverage area which increases aggregate throughput. Stations inside the common coverage area automatically associate with the AP that is less loaded and provides the best signal quality. The stations are equally divided between the APs in order to equally share the load between all APs. Efficiency is maximized because all APs are working at the same low level load. Load balancing is also known as load sharing.



**Figure A-5: Common Coverage Area of a Multi-cell Structure**



## Dynamic Rate Switching

The data rate of each station is automatically adjusted according to the received signal quality. Performance (throughput) is maximized by increasing the data rate and decreasing retransmissions. This is very important for mobile applications where the signal quality fluctuates rapidly, but less important for fixed outdoor installations where signal quality is stable.

## Media Access

When many users are located in the same area, performance becomes an issue. To address this issue, wireless LANs use the Carrier Sense Multiple Access (CSMA) algorithm with a Collision Avoidance (CA) mechanism in which each unit senses the medium before it starts to transmit.

If the medium is free for several microseconds, the unit can transmit for a limited time. If the medium is busy, the unit will back off for a random time before it senses again. Since transmitting units compete for air time, the protocol should ensure equal fairness between the stations.

## Fragmentation

Fragmentation of packets into shorter fragments adds protocol overhead and reduces protocol efficiency when no errors are expected, but reduces the time spent on retransmissions if errors are likely to occur. No fragmentation or longer fragment length adds overhead and reduces efficiency in case of errors and retransmissions (multi-path).

## Collision Avoidance

To avoid collisions with other incoming calls, each station transmits a short RTS (Request To Send) frame before the data frame. The Access Point sends back a CTS (Clear To Send) frame with permission to start the data transmission. This frame includes the time that this station is going to transmit. This frame is received by all the stations in the cell, notifying them that another unit will transmit during the following  $Xmsec$ , so they can not transmit even if the medium seems to be free (the transmitting unit is out of range).

## Channelization

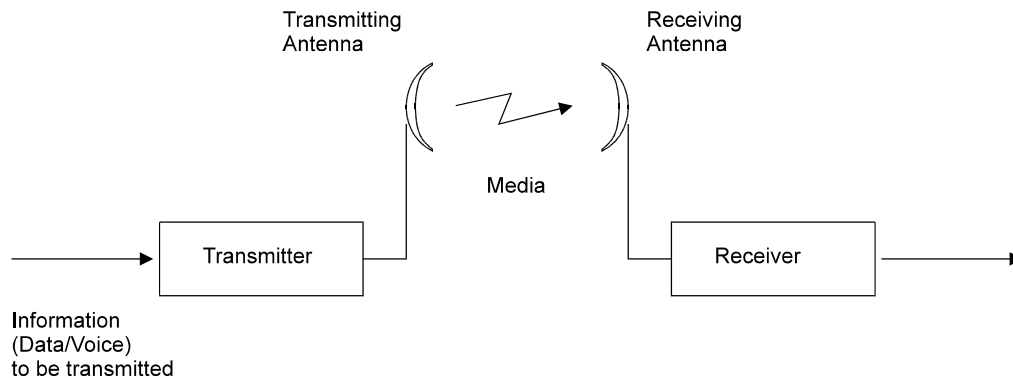
Using Frequency Hopping Spread Spectrum (FHSS), different hopping sequences are assigned to different co-located cells. Hopping sequences are designed so different cells can work simultaneously using different channels.

Since hopping sequences and hopping timing of different cells cannot be synchronized (according to FCC regulations), different cells might try to use the same channel occasionally. Then, one cell uses the channel while the other cell backs off and waits for the next hop. In the case of a very noisy environment (multiples and interference), the system must hop quickly. If the link is quiet and clean, it is better to hop slowly, reducing overhead and increasing efficiency.

# Radio Signal Propagation

This section explains and simplifies many of the terms relating to antennas and RF (Radio Frequency) used when dealing with an RF installation system.

The following diagram depicts a typical radio system:



**Figure A-6: Typical Radio System**

A radio system transmits information to the transmitter. The information is transmitted through an antenna which converts the RF signal into an electromagnetic wave. The transmission medium for electromagnetic wave propagation is free space.

The electromagnetic wave is intercepted by the receiving antenna which converts it back to an RF signal. Ideally, this RF signal is the same as that originally generated by the transmitter. The original information is then demodulated back to its original form.

## RF Terms and Definitions

### dB

The dB convention is an abbreviation for decibels. It shows the relationship between two values.

### RF Power Level

RF power level at either the transmitter output or the receiver input is expressed in Watts. It can also be expressed in dBm. The relation between dBm and Watts can be expressed as follows:

$$P_{\text{dBm}} = 10 \times \text{Log } P_{\text{mw}}$$

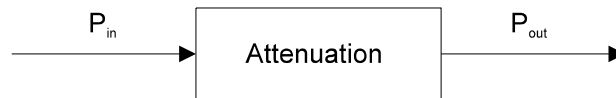
For example: 1 Watt = 1000 mW;  $P_{\text{dBm}} = 10 \times \text{Log } 1000 = 30 \text{ dBm}$

100 mW;  $P_{\text{dBm}} = 10 \times \text{Log } 100 = 20 \text{ dBm}$

For link budget calculations, the dBm convention is more convenient than the Watts convention.

### Attenuation

Attenuation (fading) of an RF signal is defined as follows:



**Figure A-7: Attenuation of an RF signal**

$P_{\text{in}}$  is the incident power level at the attenuated input

$P_{\text{out}}$  is the output power level at the attenuated output

Attenuation is expressed in dB as follows:  $P_{\text{dB}} = -10 \times \text{Log } (P_{\text{out}}/P_{\text{in}})$

For example: If, due to attenuation, half the power is lost ( $P_{\text{out}}/P_{\text{in}} = 1/2$ ), attenuation in dB is  $-10 \times \text{Log} (1/2) = 3_{\text{dB}}$

## Path Loss

Loss of power of an RF signal traveling (propagating) through space. It is expressed in dB. Path loss depends on:

- ♦ The distance between transmitting and receiving antennas
- ♦ Line of sight clearance between the receiving and transmitting antennas
- ♦ Antenna height

## Free Space Loss

Attenuation of the electromagnetic wave while propagating through space. This attenuation is calculated using the following formula:

$$\text{Free space loss} = 32.4 + 20 \times \text{Log}(F_{\text{MHz}}) + 20 \times \text{Log}(R_{\text{Km}})$$

F is the RF frequency expressed in MHz.

R is the distance between the transmitting and receiving antennas.

At 2.4 GHz, this formula is:  $100 + 20 \times \text{Log}(R_{\text{Km}})$

## Antenna Characteristics

### *Isotropic Antenna*

A hypothetical antenna having equal radiation intensity in all directions. Used as a zero dB gain reference in directivity calculation (gain).

## **Antenna Gain**

A measure of directivity. It is defined as the ratio of the radiation intensity in a given direction to the radiation intensity that would be obtained if the power accepted by the antenna was radiated equally in all directions (isotropically). Antenna gain is expressed in dBi.

## **Radiation Pattern**

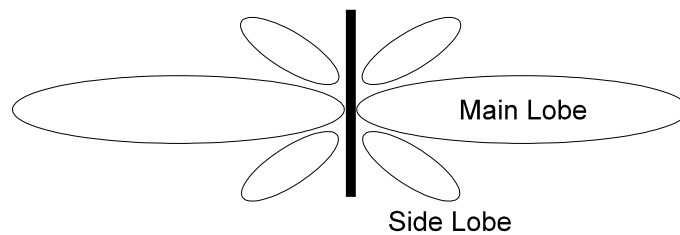
A graphical representation in either polar or rectangular coordinates of the spatial energy distribution of an antenna.

## **Side Lobes**

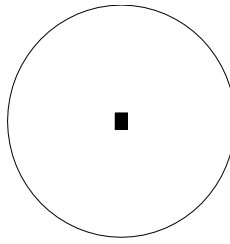
The radiation lobes in any direction other than that of the main lobe.

## **Omni-directional Antenna**

Radiates and receives equally in all directions in azimuth. The following diagram shows the radiation pattern of an omni-directional antenna with its side lobes in polar form.



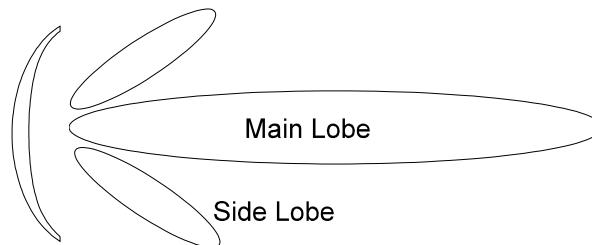
**Figure A-8: Side View**



**Figure A-9: Top View**

### ***Directional Antenna***

Radiates and receives most of the signal power in one direction. The following diagram shows the radiation pattern of a directional antenna with its side lobes in polar form:



**Figure A-10: Radiation Pattern of Directional Antenna**

### ***Antenna Beamwidth***

The directiveness of a directional antenna. Defined as the angle between two half-power (-3 dB) points on either side of the main lobe of radiation.

## **System Characteristics**

### ***Receiver Sensitivity***

The minimum RF signal power level required at the input of a receiver for certain performance (e.g. BER).

### **EIRP (Effective Isotropic Radiated Power)**

The antenna transmitted power. Equal to the transmitted output power minus cable loss plus the transmitting antenna gain.

$P_{out}$	Output power of transmitted in dBm
$C_t$	Transmitter cable attenuation in dB
$G_t$	Transmitting antenna gain in dBi
$G_r$	Receiving antenna gain in dBi
$P_l$	Path loss in dB
$C_r$	Receiver cable attenuation is dB
$S_i$	Received power level at receiver input in dBm
$P_s$	Receiver sensitivity is dBm

$$S_i = P_{out} - C_t + G_t - P_l + G_r - C_r$$

$$EIRP = P_{out} - C_t + G_t$$

#### **Example:**

##### **Link Parameters:**

Frequency: 2.4 GHz

$P_{out} = 4$  dBm (2.5 mW)

Tx and Rx cable length ( $C_t$  and  $C_r$ ) = 10 m. cable type RG214 (0.6 dB/meter)

Tx and Rx antenna gain ( $G_t$  and  $G_r$ ) = 18 dBi

Distance between sites = 3 Km

Receiver sensitivity ( $P_s$ ) = -84 dBm

Link Budget Calculation



$$\text{EIRP} = P_{\text{out}} - C_t + G_t = 16 \text{ dBm}$$

$$P_l = 32.4 + 20 \times \log(\text{FMHz}) + 20 \times \log(\text{Rkm}) \cong 110 \text{ dB}$$

$$S_i = \text{EIRP} - P_l + G_r - C_r = -82 \text{ dBm}$$

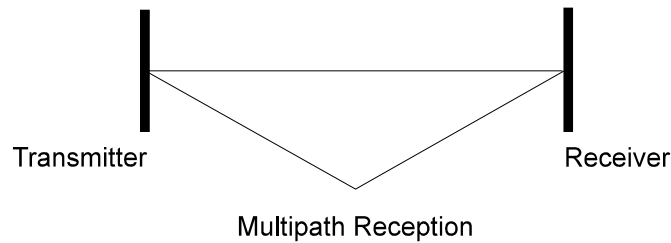
In conclusion, the received signal power is above the sensitivity threshold, so the link should work. The problem is that there is only a 2 dB difference between received signal power and sensitivity. Normally, a higher margin is desirable due to fluctuation in received power as a result of signal fading.

## Signal Fading

Fading of the RF signal is caused by several factors:

### ♦ Multipath

The transmitted signal arrives at the receiver from different directions, with different path lengths, attenuation and delays. The summed signal at the receiver may result in an attenuated signal.



**Figure A-11: Multipath Reception**

### ♦ Bad Line of Sight

An optical line of sight exists if an imaginary straight line can connect the antennas on either side of the link.

Radio wave clear line of sight exists if a certain area around the optical line of sight (Fresnel zone) is clear of obstacles. A bad line of sight exists if the first Fresnel zone is obscured.

### ♦ Link Budget Calculations

- ◆ Weather conditions (Rain, wind, etc.)

At high rain intensity (150 mm/hr), the fading of an RF signal at 2.4 GHz may reach a maximum of 0.02 dB/Km

Wind may cause fading due to antenna motion.

- ◆ **Interference**

Interference may be caused by another system on the same frequency range, external noise, or some other co-located system.

## **The Line of Sight Concept**

An optical line of sight exists if an imaginary straight line can be drawn connecting the antennas on either side of the link.

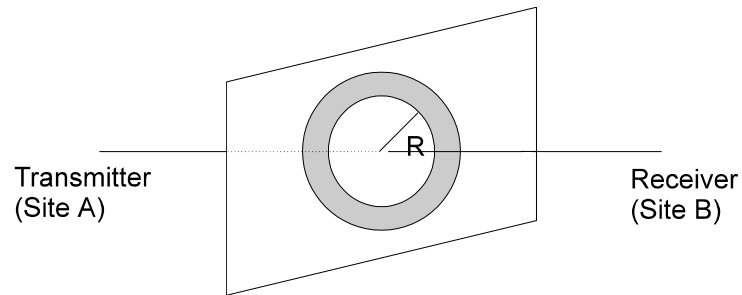
### ***Clear Line of Sight***

A clear line of sight exists when no physical objects obstruct viewing one antenna from the location of the other antenna.

A radio wave clear line of sight exists if a defined area around the optical line of sight (Fresnel Zone) is clear of obstacles.

## Fresnel Zone

The Fresnel zone is the area of a circle around the line of sight.  
The Fresnel Zone is defined as follows:



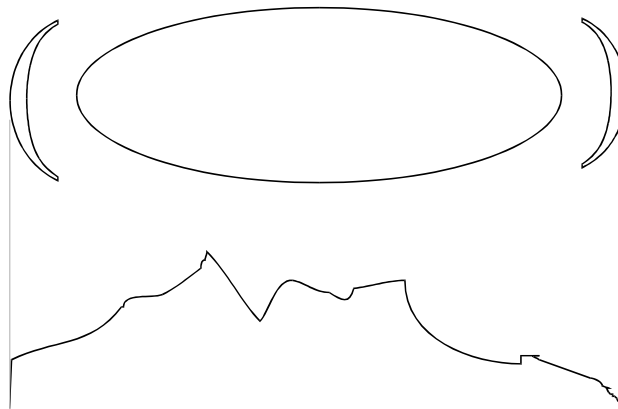
**Figure A-12: Fresnel Zone**

$$R = \frac{1}{2} \sqrt{\lambda \times D}$$

R: radius of the first Fresnel zone

$\lambda$ : wavelength

D: distance between sites



**Figure A-13: Fresnel Zone Clear of Obstacles**

When at least 80% of the first Fresnel Zone is clear of obstacles, propagation loss is equivalent to that of free space.

# IEEE 802.11 Technical Tutorial

The purpose of this section is to give technical readers a basic overview of the new IEEE 802.11 Standard, enabling them to understand the basic concepts, principles of operation, and the reasons behind some of the features and/or components of the Standard.

The document does not cover the entire Standard and does not provide enough information for the reader to implement an 802.11-compliant device (for this purpose the reader should refer to the standard).

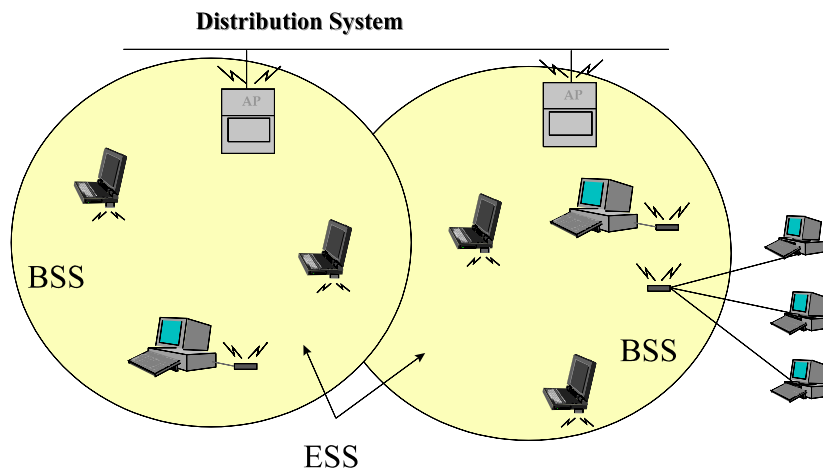
## Architecture Components

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell (called Basic Service Set, or BSS, in the 802.11 nomenclature) is controlled by a Base Station (called Access Point or, in short, AP).

Although a wireless LAN may be formed by a single cell, with a single Access Point, (and as will be described later, it can also work without an Access Point), most installations will be formed by several cells, where the Access Points are connected through some kind of backbone (called Distribution System or DS). This backbone is typically Ethernet but, in some cases, might be wireless itself.

The whole interconnected wireless LAN, including the different cells, their respective Access Points and the Distribution System, is seen as a single 802 network to the upper layers of the OSI model and is known in the Standard as the Extended Service Set (ESS).

The following diagram shows a typical 802.11 LAN including the components described above:



**Figure A-14: Typical 802.11 LAN**

The standard also defines the concept of a Portal. A portal is a device that interconnects between an 802.11 and another 802 LAN. This concept is an abstract description of part of the functionality of a “translation bridge”.

Even though the standard does not necessarily require it, typical installations will have the AP and the Portal on a single physical entity. This is also the case with Alvarion's AP which provides both functions.

## IEEE 802.11 Layers Description

As in any 802.x protocol, the IEEE 802.11 protocol covers the Media Access Control Layer (MAC) and Physical Layer (PHY). The Standard currently defines a single MAC which interacts with three PHYs (all of them running at 1 or 2 Mbit/s) as follows:

- ◆ Frequency Hopping Spread Spectrum (FHSS) in the 2.4 GHz Band

- ◆ Direct Sequence Spread Spectrum (DSSS) in the 2.4 GHz Band, and
- ◆ InfraRed

802.2			Data Link Layer
802.11 MAC			
FH	DS	IR	PHY Layer

Beyond the standard functionality usually performed by MAC Layers, the 802.11 MAC performs other functions that are typically related to upper layer protocols, such as Fragmentation, Packet Retransmissions, and Acknowledges.

## The MAC Layer

The MAC Layer defines two different access methods, the Distributed Coordination Function and the Point Coordination Function:

### The Basic Access Method: CSMA/CA

The basic access mechanism, called the **Distributed Coordination Function**, is basically a Carrier Sense Multiple Access with Collision Avoidance mechanism (known as **CSMA/CA**). CSMA protocols are well-known in the industry, the most popular being Ethernet, which is a CSMA/ CD protocol (CD standing for Collision Detection).

A CSMA protocol works as follows: A station desiring to transmit senses the medium. If the medium is busy (i.e. some other station is transmitting) then the station defers its transmission to a later time. If the medium seems free then the station is allowed to transmit.

These kinds of protocols are very effective when the medium is not heavily loaded since it allows stations to transmit with minimum delay. But there is always a chance of two or more stations simultaneously sensing the medium as being free and transmitting at the same time, causing a collision.

These collision situations must be identified so the MAC layer can retransmit the packet itself, not by the upper layers, to avoid significant delay. In the Ethernet case, a collision is recognized by the transmitting stations which listen while transmitting and go into a retransmission phase based on an **exponential random back-off** algorithm.

While these Collision Detection Mechanisms are a good idea on a wired LAN, they cannot be used on a wireless LAN environment for two main reasons:

- ◆ Implementing a Collision Detection Mechanism would require the implementation of a Full-Duplex radio capable of transmitting and receiving at the same time, an approach that would increase the price significantly.
- ◆ In a wireless environment we cannot assume that all stations can hear each other (a basic assumption of the Collision Detection scheme), and the fact that a station wants to transmit and senses the medium as free doesn't necessarily mean that the medium is free around the receiver's area.

In order to overcome these problems, 802.11 uses a Collision Avoidance (CA) mechanism together with a Positive Acknowledge scheme, as follows:

A station wanting to transmit senses the medium. If the medium is busy then it delays. If the medium is free for a specified time (called Distributed Inter Frame Space (DIFS) in the standard), then the station is allowed to transmit.



The receiving station checks the CRC of the received packet and sends an acknowledgment packet (ACK). Receipt of the acknowledgment indicates to the transmitter that no collision occurred. If the sender does not receive the acknowledgment, then it retransmits the fragment until it either receives acknowledgment or is thrown away after a given number of retransmissions.

## Virtual Carrier Sense

In order to reduce the probability of two stations colliding because they cannot hear each other, the standard defines a Virtual Carrier Sense mechanism:

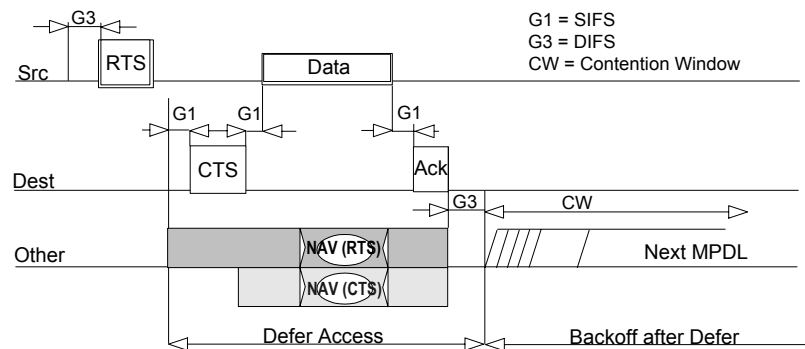
A station wanting to transmit a packet first transmits a short control packet called **RTS** (Request To Send), which includes the source, destination, and the duration of the following transaction (i.e. the packet and the respective **ACK**), the destination station responds (if the medium is free) with a response control Packet called **CTS** (Clear to Send), which includes the same duration information.

All stations receiving either the RTS or the CTS, set their Virtual Carrier Sense indicator (called NAV, for Network Allocation Vector), for the given duration, and use this information together with the Physical Carrier Sense when sensing the medium.

This mechanism reduces the probability of a collision on the receiver area by a station that is “hidden” from the transmitter to the short duration of the RTS transmission because the station hears the CTS and “reserves” the medium as busy until the end of the transmission. The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledging station).

It should also be noted that, due to the fact that the RTS and CTS are short frames, the mechanism also reduces the overhead of collisions, since these are recognized faster than if the whole packet was to be transmitted. (This is true if the packet is significantly bigger than the RTS, so the standard allows for short packets to be transmitted without the RTS/CTS transmission. This is controlled per station by a parameter called RTS Threshold).

The following diagrams show an exchange between stations A and B, and the NAV setting of their neighbors:



**Figure A-15: Transaction Between Stations A and B**

The NAV State is combined with the physical carrier sense to indicate the busy state of the medium.

## MAC Level Acknowledgments

As mentioned earlier in this document, the MAC layer performs Collision Detection by expecting the reception of an acknowledge to any transmitted fragment (Packets that have more than one destination, such as Multicasts, are not acknowledged.)

## Fragmentation and Reassembly

Typical LAN protocols use packets several hundred bytes long (the longest Ethernet packet could be up to 1518 bytes long).

There are several reasons why it is preferable to use smaller packets in a wireless LAN environment:

- ◆ Due to the higher Bit Error Rate of a radio link, the probability of a packet getting corrupted increases with the packet size.
- ◆ In case of packet corruption (either due to collision or noise), the smaller the packet, the less overhead it causes to retransmit it.
- ◆ On a Frequency Hopping system, the medium is interrupted periodically for hopping (in our case every 20 milliseconds), so, the smaller the packet, the smaller the chance that the transmission will be postponed after dwell time.

However, it doesn't make sense to introduce a new LAN protocol that cannot deal with packets 1518 bytes long which are used on Ethernet, so the committee decided to solve the problem by adding a simple fragmentation/ re-assembly mechanism at the MAC Layer.

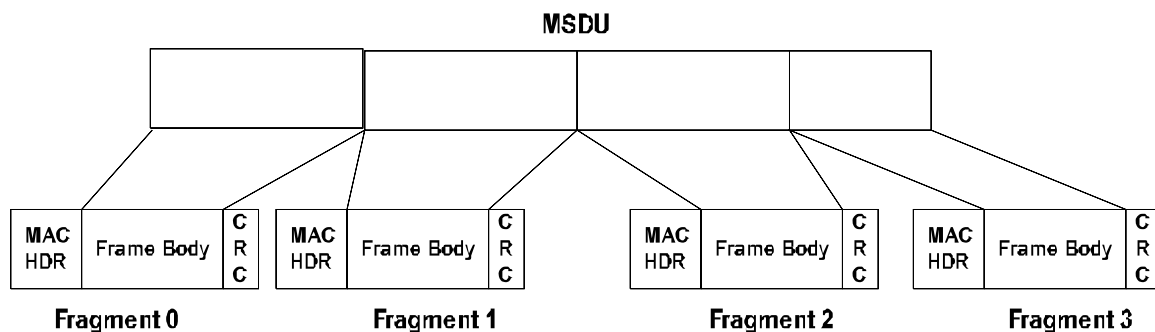
The mechanism is a simple Send-and-Wait algorithm, where the transmitting station is not allowed to transmit a new fragment until one of the following happens:

Receives an ACK for the said fragment, or

Decides that the fragment was retransmitted too many times and drops the whole frame.

It should be noted that the standard does allow the station to transmit to a different address between retransmissions of a given fragment. This is particularly useful when an AP has several outstanding packets to different destinations and one of them does not respond.

The following diagram shows a frame (MSDU) being divided to several fragments (MPDUs):



**Figure A-16: Frame Fragmentation**

## Inter-Frame Spaces

The Standard defines 4 types of Inter Frame Spaces, which are used to provide different priorities:

- ◆ SIFS – Short Inter Frame Space, separates transmissions belonging to a single dialog (e.g. Fragment-Ack), and is the minimum Inter Frame Space. There is always at most one single station to transmit at any given time, therefore giving it priority over all other stations. This value is a fixed value per PHY and is calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet. On the 802.11 FH PHY this value is set to 28 microseconds
- ◆ PIFS – Point Coordination IFS, is used by the Access Point (or Point Coordinator, as called in this case), to gain access to the medium before any other station. This value is SIFS plus a Slot Time (defined in the following paragraph), i.e. 78 microseconds.

- ♦ DIFS – Distributed IFS, is the Inter Frame Space used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time, i.e. 128 microseconds.
- ♦ EIFS – Extended IFS, which is a longer IFS used by a station that has received a packet that it could not understand. This is needed to prevent the station (which could not understand the duration information for the Virtual Carrier Sense) from colliding with a future packet belonging to the current dialog.

## Exponential Back-off Algorithm

**Back-off** is a well known method used to resolve contention between different stations wanting to access the medium. The method requires each station to choose a Random Number (n) between 0 and a given number, and wait for this number of Slots before accessing the medium, always checking if a different station has accessed the medium before.

The **Slot Time** is defined in such a way that a station will always be capable of determining if another station has accessed the medium at the beginning of the previous slot. This reduces collision probability by half.

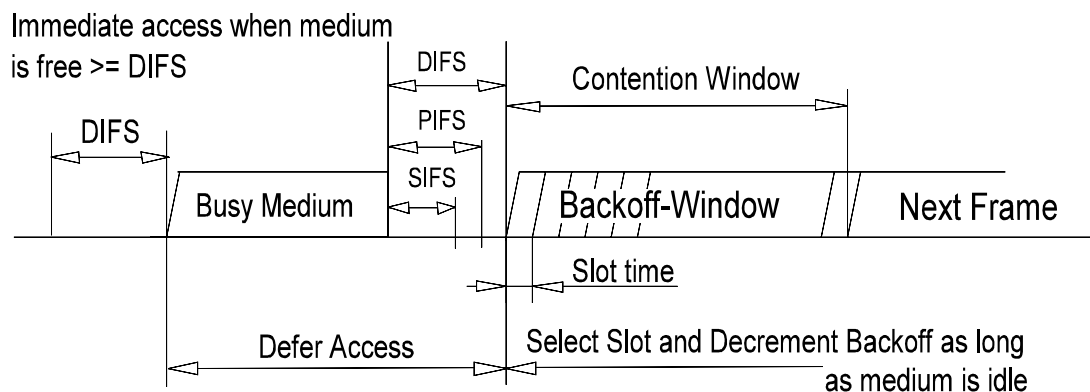
Exponential Back-off means that each time the station chooses a slot and happens to collide, it will increase the maximum number for the random selection exponentially.

The 802.11 standard defines an **Exponential Back-off Algorithm**, that must be executed in the following cases:

- ♦ When the station senses the medium before the first transmission of a packet, and the medium is busy
- ♦ After each retransmission, and
- ♦ After a successful transmission

The only case when this mechanism is not used is when the station decides to transmit a new packet and the medium has been free for more than DIFS.

The following figure shows a schematic of the access mechanism:



**Figure A-17: Access Mechanism**

## How Does a Station Join an Existing Cell

When a station wants to access an existing BSS (either after power-up, sleep mode, or just entering the BSS area), the station needs to get synchronization information from the Access Point (or from the other stations when in ad-hoc mode, which will be discussed later).

The station can get this information by one of two means:

- ◆ **Passive Scanning:** In this case the station just waits to receive a Beacon Frame from the AP, (the beacon frame is a frame sent out periodically by the AP containing synchronization information), or

- ◆ **Active Scanning:** In this case the station tries to locate an Access Point by transmitting Probe Request Frames, and waits for Probe Response from the AP.

Both methods are valid. A method is chosen according to the power consumption/performance trade-off.

## **The Authentication Process**

Once the station has located an Access Point, and decides to join its BSS, it goes through the Authentication Process. This is the interchange of information between the AP and the station, where each side proves the knowledge of a given password.

## **The Association Process**

Once the station is authenticated, it then starts the Association Process, which is the exchange of information about the station and BSS capabilities, and which allows the DSS (the set of APs) to know about the current position of the station). A station is capable of transmitting and receiving data frames only after the association process is completed.

## **Roaming**

Roaming is the process of moving from one cell (or BSS) to another without losing connection. This function is similar to the cellular phones' handover, with two main differences:

On a packet-based LAN system, the transition from cell to cell may be performed between packet transmissions, as opposed to telephony where the transition may occur during a phone conversation, this makes the LAN roaming a little easier, but

On a voice system, a temporary disconnection may not affect the conversation, while in a packet-based environment it significantly reduces performance because retransmission is then performed by the upper layer protocols.

The 802.11 standard does not define how roaming should be performed, but defines the basic tools. These include active/passive scanning, and a re-association process, where a station which is roaming from one Access Point to another becomes associated with the new one<sup>1</sup>.

## Keeping Synchronization

Stations need to keep synchronization, which is necessary for keeping hopping synchronized, and other functions like Power Saving. On an infrastructure BSS, this is achieved by all the stations updating their clocks according to the AP's clock, using the following mechanism:

The AP periodically transmits frames called Beacon Frames. These frames contain the value of the AP's clock at the moment of transmission (note that this is the moment when transmission actually occurs, and not when it is put in the queue for transmission. Since the Beacon Frame is transmitted using CSMA rules, transmission may be delayed significantly).

The receiving stations check the value of their clocks at the moment the signal is received, and correct it to keep in synchronization with the AP's clock. This prevents clock drifting which could cause loss of synch after a few hours of operation.

---

<sup>1</sup>The BreezeNET product line provides a patented enhanced roaming mechanism which allows stations to roam at speeds of 60 Km/h without losing or duplicating packets.



## Security

Security is one of the first concerns that people have when deploying a wireless LAN. The 802.11 committee has addressed the issue by providing what is referred to as WEP (Wired Equivalent Privacy).

Users are primarily concerned that an intruder should not be able to:

- ◆ Access the Network resources by using similar wireless LAN equipment
- ◆ Capture wireless LAN traffic (eavesdropping)

## Preventing Access to Network Resources

This is done by the use of an Authentication mechanism where a station needs to prove knowledge of the current key. This is very similar to Wired LAN privacy, in the sense that an intruder needs to enter the premises (by using a physical key) in order to connect his workstation to the wired LAN.

## Eavesdropping

Eavesdropping is prevented by using the WEP algorithm which is a pseudo-random number generator initialized by a shared secret key. This PRNG outputs a key sequence of pseudo-random bits equal in length to the largest possible packet which is combined with the outgoing/incoming packet producing the packet transmitted in the air.

The WEP is a simple algorithm based on RSA's RC4 which has the following properties:

- ◆ Reasonably Strong: Brute-force attack to this algorithm is difficult because every frame is sent with an Initialization Vector which restarts the PRNG for each frame.
- ◆ Self Synchronizing: The algorithm re-synchronizes for each message. This is necessary in order to work in a connection-less environment, where packets may get lost (as any LAN).

## Power Saving

Wireless LANs are typically related to mobile applications. In this type of application, battery power is a scarce resource. This is the reason why the 802.11 standard directly addresses the issue of Power Saving and defines an entire mechanism which enables stations to go into sleep mode for long periods of time without losing information.

The main idea behind the Power Saving Mechanism is that the AP maintains a continually updated record of the stations currently working in Power Saving mode, and buffers the packets addressed to these stations until either the stations specifically request the packets by sending a polling request, or until they change their operation mode.

As part of its Beacon Frames, the AP also periodically transmits information about which Power Saving Stations have frames buffered at the AP, so these stations wake up in order to receive the Beacon Frame. If there is an indication that there is a frame stored at the AP waiting for delivery, then the station stays awake and sends a Polling message to the AP to get these frames.

Multicasts and Broadcasts are stored by the AP, and transmitted by the AP at pre-defined intervals (called DTIM), all stations - both stations working in Power Saving mode and stations working in Normal mode, will be awake at that period and will receive this kind of frames.

Unicasts are stored by the AP, and transmitted at station-defined intervals (called Listen Intervals), when all stations who wish to receive this kind of frames are awake. Unicast frames are transmitted upon request only, whereas, Multicast frames are transmitted automatically at every DTIM interval.

**NOTE:**

Unicast frames can be also polled by the stations at the DTIM intervals.

## Frame Types

There are three main types of frames:

- ◆ Data Frames: which are used for data transmission
- ◆ Control Frames: which are used to control access to the medium (e.g. RTS, CTS, and ACK), and
- ◆ Management Frames: which are frames that are transmitted in the same manner as data frames to exchange management information, but are not forwarded to upper layers (e.g. beacon frames).

Each frame type is subdivided into different Subtypes, according to its specific function.

## Frame Formats

All 802.11 frames are composed of the following components:

Preamble	PLCP Header	MAC Data	CRC
----------	-------------	----------	-----

### Preamble

This is PHY dependent, and includes:

- ◆ Synch: An 80-bit sequence of alternating zeros and ones, which is used by the PHY circuitry to select the appropriate antenna (if diversity is used), and to reach steady-state frequency offset correction and synchronization with the received packet timing.
- ◆ SFD: A Start Frame delimiter which consists of the 16-bit binary pattern 0000 1100 1011 1101, which is used to define frame timing.

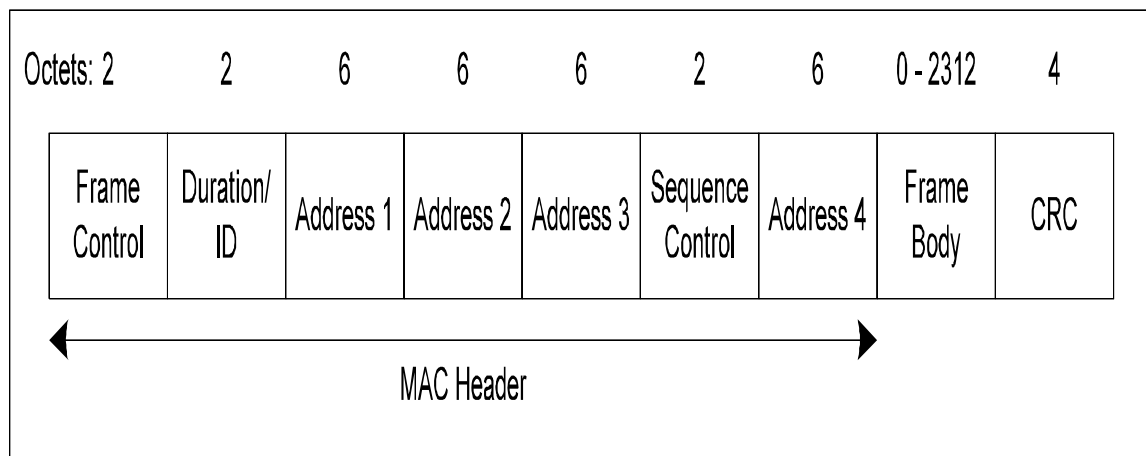
## PLCP Header

The PLCP Header is always transmitted at 1 Mbit/s and contains Logical information used by the PHY Layer to decode the frame. It consists of:

- ◆ PLCP\_PDU Length Word: which represents the number of bytes contained in the packet. This is useful for the PHY to correctly detect the end of packet.
- ◆ PLCP Signaling Field: which currently contains only the rate information, encoded in 0.5 Mbps increments from 1 Mbit/s to 4.5 Mbit/s.
- ◆ Header Error Check Field: Which is a 16 Bit CRC error detection field.

## MAC Data

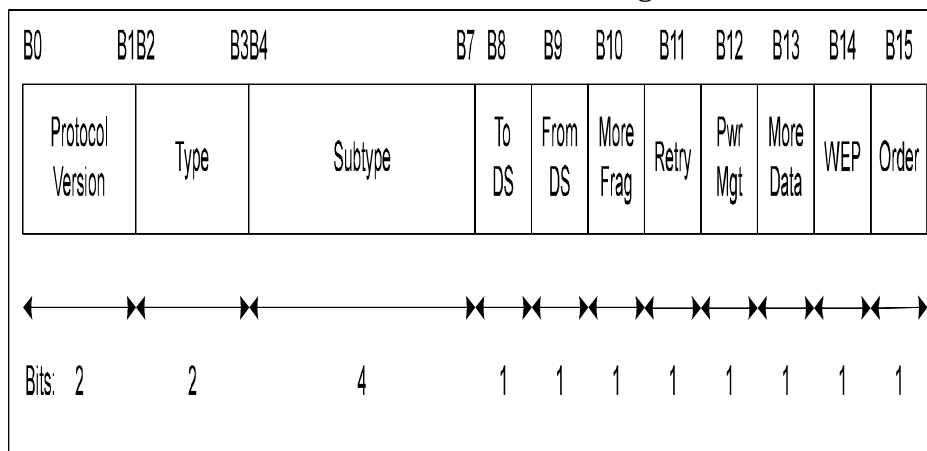
The following figure shows the general MAC Frame Format. Part of the fields are only present in part of the frames as described later.



**Figure A-18: MAC Frame Format**

## Frame Control Field

The Frame Control field contains the following information:



**Figure A-19: Frame Control Field**

## Protocol Version

This field consists of 2 bits which are invariant in size and placement across following versions of the 802.11 Standard, and will be used to recognize possible future versions. In the current version of the standard the value is fixed as 0.

## **Type and Subtype**

These 6 bits define the Type and SubType of the frame as indicated in the following table:

Type Value b3-b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Association Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-0001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS

Type Value b3-b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
10	Data	0000-1111	Reserved

### **ToDS**

This bit is set to 1 when the frame is addressed to the AP for forwarding to the Distribution System (including the case where the destination station is in the same BSS, and the AP is to relay the frame).

The Bit is set to 0 in all other frames.

***FromDS***

This bit is set to 1 when the frame is received from the Distribution System.

***More Fragments***

This bit is set to 1 when there are more fragments belonging to the same frame following the current fragment.

***Retry***

This bit indicates that this fragment is a retransmission of a previously transmitted fragment. This is used by the receiver station to recognize duplicate transmissions of frames that may occur when an Acknowledgment packet is lost.

***Power Management***

This bit indicates the Power Management mode that the station will be in after the transmission of this frame. This is used by stations which are changing state either from Power Save to Active or vice versa.

***More Data***

This bit is used for Power Management as well as by the AP to indicate that there are more frames buffered for this station. The station may decide to use this information to continue polling or even changing to Active mode.

***WEP***

This bit indicates that the frame body is encrypted according to the WEP algorithm



## **Order**

This bit indicates that this frame is being sent using the Strictly-Ordered service class<sup>2</sup>.

## **Duration/ID**

This field has two meanings depending on the frame type:

- ◆ In Power-Save Poll messages this is the Station ID
- ◆ In all other frames this is the duration value used for the NAV Calculation.

## **Address Fields**

A frame may contain up to 4 Addresses depending on the ToDS and FromDS bits defined in the Control Field, as follows:

- ◆ Address-1 is always the Recipient Address (i.e. the BSS station that is the immediate recipient of the packet). If ToDS is set, this is the AP Address; if ToDS is not set, then this is the address of the end-station.
- ◆ Address-2 is always the Transmitter Address (i.e. the station which is physically transmitting the packet). If FromDS is set, this is the AP address; if it is not set, then it is the Station address.
- ◆ Address-3 is in most cases the remaining, missing address. On a frame with FromDS set to 1, Address-3 is the original Source Address; if the frame has the ToDS set, then Address 3 is the destination Address.

---

<sup>2</sup> The Strictly-Ordered Service Class is defined for users that cannot accept change of ordering between Unicast Frames and Multicast Frames (ordering of Unicast frames to a specific address is always maintained). The only known protocol that would need this service class is DEC's LAT.

- ◆ Address-4 is used in special cases where a Wireless Distribution System is used, and the frame is being transmitted from one Access Point to another. In such cases, both the ToDS and FromDS bits are set, so both the original Destination and the original Source Addresses are missing.

The following Table summarizes the usage of the different Addresses according to ToDS and FromDS bits setting:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

### **Sequence Control**

The Sequence Control Field is used to represent the order of different fragments belonging to the same frame, and to recognize packet duplications. It consists of two subfields, Fragment Number and Sequence Number, which define the frame and the number of the fragment in the frame.

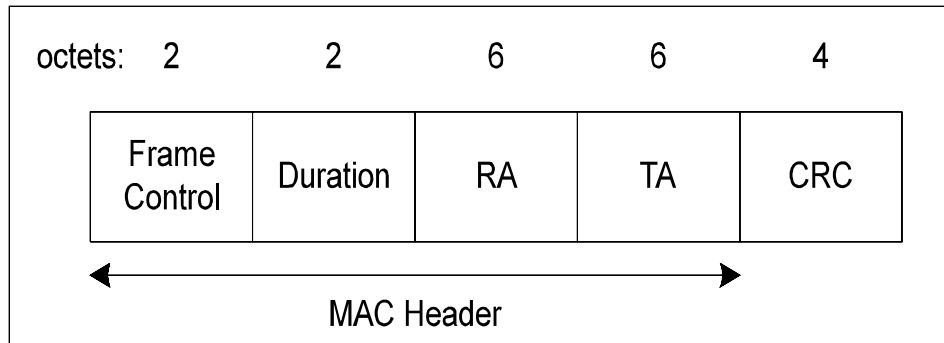
### **CRC**

The CRC is a 32-bit field containing a 32-bit Cyclic Redundancy Check (CRC).

## Most Common Frame Formats

### RTS Frame Format

The RTS frame looks as follows:



**Figure A-20: RTS Frame Format**

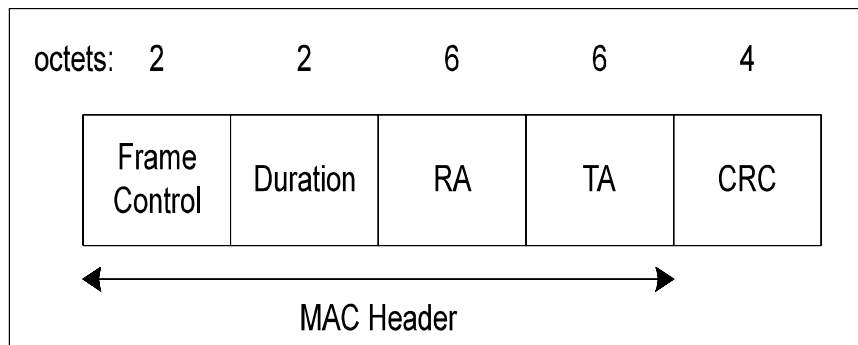
The RA of the RTS frame is the address of the STA on the wireless medium that is the intended immediate recipient of the next Data or Management frame.

The TA is the address of the STA transmitting the RTS frame.

The Duration value is the time, in microseconds, required to transmit the next Data or Management frame, plus one CTS frame, plus one ACK frame, plus three SIFS intervals.

## CTS Frame Format

The CTS frame looks as follows:



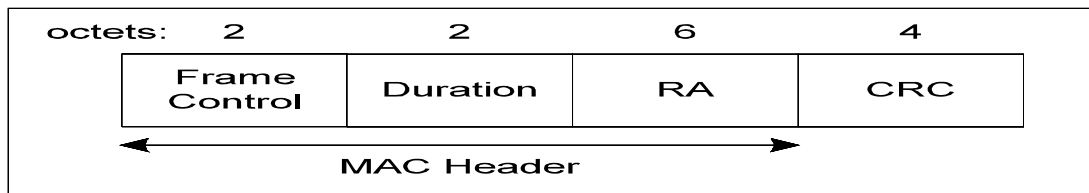
**Figure A-21: CTS Frame**

The Receiver Address (RA) of the CTS frame is copied from the Transmitter Address (TA) field of the immediately previous RTS frame to which the CTS is a response.

The Duration value is the value obtained from the Duration field of the immediately previous RTS frame, minus the time, in microseconds, required to transmit the CTS frame and its SIFS interval.

## ACK Frame Format

The ACK frame looks as follows:



**Figure A-22: ACK Frame Format**

The Receiver Address of the ACK frame is copied from the Address 2 field of the immediately previous frame.

If the More Fragment bit was set to 0 in the Frame Control field of the previous frame, the Duration value is set to 0, otherwise the Duration value is obtained from the Duration field of the previous frame, minus the time, in microseconds, required to transmit the ACK frame and its SIFS interval.

## **Point Coordination Function (PCF)**

Beyond the basic Distributed Coordination Function, there is an optional Point Coordination Function, which may be used to implement time-bounded services, like voice or video transmission. This Point Coordination Function makes use of the higher priority that the Access Point may gain by the use of a smaller Inter Frame Space (PIFS).

By using this higher priority access, the Access Point issues polling requests to the stations for data transmission, hence controlling medium access. To still enable regular stations to access the medium, there is a provision that the Access Point must leave enough time for Distributed Access in between the PCF.

## Ad-Hoc Networks

In certain circumstances, users may wish to build up wireless LAN networks without an infrastructure (more specifically without an Access Point). This may include file transfer between two notebook users, co-workers meeting outside the office, etc.

The 802.11 standard addresses this need by the definition of an “ad-hoc” mode of operation. In this case, there is no Access Point and part of its functionality is performed by the end-user stations (such as Beacon Generation, synchronization, etc.). Other AP functions are not supported (such as frame-relaying between two stations not in range, or Power Saving).